# A SZEGEDI TUDOMÁNYEGYETEM ADATVÉDELMI SZABÁLYZATA

**Szeged, 2024. április 29.**

**SZ-VIII/2023/2024.**

## Tartalom

## PREAMBULUM

A Szegedi Tudományegyetem (a továbbiakban: Egyetem) Szenátusa átérezve az Egyetem feladatellátásából származó adatvédelmi felelősség súlyát, a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló az Európai Parlament és a Tanács (EU) 2016/679 rendelete (a továbbiakban: GDPR), valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) alapján valamennyi szervezeti egységére vonatkozóan az adatkezelés általános rendjére az alábbi Adatvédelmi Szabályzatot (a továbbiakban: Szabályzatot) alkotja.

## I. ÁLTALÁNOS RENDELKEZÉSEK

### *A Szabályzat hatálya*

1. §

(1) Jelen Szabályzat meghatározza az Egyetem személyes adatok kezelésével és adatbiztonsággal kapcsolatos legfontosabb feladatait, az érintetteket megillető jogokat, az adatkezelés és adatvédelem szervezet- és eljárásrendszerét.
(2) Amennyiben vita merül fel a Szabályzat hatályát illetően, akkor a vita feloldására, a vita írásbeli jelzésétől számított lehető legrövidebb időn belül, legkésőbb 10 munkanapon belül az Egyetemi főtitkár (a továbbiakban: Főtitkár) köteles döntést hozni. A vita eldöntésében az Egyetem adatvédelmi tisztviselője (a továbbiakban: DPO), valamint a Jogi és Igazgatási Igazgatóság igazgatója (a továbbiakban: JII vezetője) véleménye kikérhető.

### *Személyi hatály*

2. §

(1) A Szabályzat személyi hatálya kiterjed minden olyan természetes személyre, aki az Egyetem nevében, annak felkérésére, utasítására, munkaköri feladatának teljesítése céljából vagy az Egyetemmel kötött megbízási szerződés vagy más polgári jogi szerződés teljesítése céljából személyes adatot kezel, vagy ő az adatkezelés érintettje, függetlenül állampolgárságától.
(2) A (1) bekezdésre figyelemmel a Szabályzat személyi hatálya kiterjed különösen:
a) az Egyetem, mint adatkezelő vagy adatfeldolgozó adatkezelési tevékenységeinek megvalósításában, a közreműködés időtartamától és gyakoriságától függetlenül közreműködő valamennyi szervezeti egységének
aa) munkavállalóira,
ab) vele egészségügyi szolgálati jogviszonyban állókra,
ac) köznevelési foglalkoztatotti jogviszonyban állókra,
ad) megbízottjaira,
ae) szolgáltatóira.
b) az Egyetem mint adatkezelő által megvalósított adatkezelések érintettjeire, így különösen
ba) az Egyetem, mint munkáltató nevében munkáltatói jogokat gyakorló személyekre,
bb) az Egyetemmel munkajogi jogviszonyban állókra,

bc) az Egyetemen egészségügyi szolgálati jogviszonyban állókra,
bd) az Egyetemmel tanulói, hallgatói, felnőttképzési, vendéghallgatói, továbbképzési, valamint doktorjelölti jogviszonyban álló személyekre,
be) az Egyetemmel megbízási vagy más, munkavégzésre irányuló egyéb jogviszonyban álló személyekre (különösen a köznevelési foglalkoztatti jogviszonyban dolgozókra, óraadó oktatókra, kutatókra, tanárokra, közérdekű önkéntes szerződés, egyéni közreműködői szerződés, vállalkozói szerződés, szolgáltatási szerződés, hallgatói munkaszerződés, doktorandusz szerződés keretében az Egyetemen munkát végző személyekre),
bf) a Professor Emeritus címmel rendelkező, továbbá foglalkoztatási jogviszonyban nem álló, egyéb címmel rendelkező személyekre, továbbá
bg) akik az Egyetemmel nem állnak a (2) bekezdés ba)-bf) pontjai szerinti jogviszonyban, azonban mégis kapcsolatba kerülnek az Egyetemmel, különösen az alábbiak szerint
1. az Egyetemen lefolytatott doktori képzésben, doktori fokozatszerzési eljárásban, illetve habilitációs eljárásban vesznek részt,
2. tanulói, hallgatói, felnőttképzési, vendéghallgatói, továbbképzési, valamint doktorjelölti jogviszony létesítése céljából adataikat az Egyetem kezeli (pl.: felvételizők, vagy tanfolyamra, képzésre jelentkezők, érdeklődők),
3. személyes adataikat jogszabályi előírás folytán, illetve más jogalap mentén az Egyetem a jogviszony megszűnését követően, vagy esemény, program elteltét követően kezeli a megőrzési idő alatt,
4. az Egyetem könyvtári rendszerét használó személyek,
5. az Egyetem infrastruktúráját használó személyek,
6. az Egyetem Klinikai Központjában (a továbbiakban: KK) ellátott betegek és hozzátartozóik,
7. az Egyetem által akár időszakos, akár állandó jelleggel működtetett bármilyen szolgáltatást igénybe vevő személyek,
8. az Egyetem bármelyik szervezeti egységéhez álláspályázatot, ajánlatot benyújtó személyek,
9. az Egyetem bármelyik szervezeti egységéhez panaszt, közérdekű bejelentést, integritássértést, egyéb tárgykörű észrevételt megfogalmazó, közérdekű adatigénylést kérő, illetve információt kérő személyek.

(3) A szervezeti egységek vezetői – ideértve a Hallgatói Önkormányzat és a Doktorandusz Önkormányzat elnökeit is – saját hatáskörükben kötelesek gondoskodni jelen Szabályzatban foglaltak betartásáról és betartatásáról.

### *Tárgyi hatály*

*[Kapcsolódó jogi háttér: Magyarország Alaptörvénye (a továbbiakban: Alaptörvény) VI. cikk (3) bekezdés]*

3. §

(1) A Szabályzat tárgyi hatálya a területi és személyi hatály keretei között folytatott valamennyi személyes adattal kapcsolatos adatkezelésre kiterjed, függetlenül attól, hogy e tevékenységben az Egyetem adatkezelőként vagy adatfeldolgozói minőségében vesz részt, illetve, hogy az adatkezelés teljesen vagy részben automatizált módon, informatikai eszközzel, vagy manuális módon papíralapon, továbbá, hogy a személyes adat kezelése adatállományban vagy azon kívül történik.

(2) A Szabályzat tárgyi hatálya nem terjed ki az információszabadság kérdéseire, e témakörben az Egyetem Szenátusa önálló szabályzatot fogad el, amely rendezi a közérdekű adatok, illetve a közérdekből nyilvános adatok megismerésének szabályait és az Egyetem ezzel kapcsolatos közzétételi kötelezettségét, valamint tájékoztatási kötelezettségét.
(3) Az adatkezelési tevékenységek megvalósulási helye, módja az Egyetem adatkezelői szervezeti egységei adatkezelési tevékenységek nyilvántartásában követhető nyomon. Az adatkezelési tevékenységek nyilvántartásának meglétét és tartalmát a DPO ellenőrzi.

### *A Szabályzat jogszabályi háttere*

4. §

(1) A Szabályzat főbb jogszabályi hátterét és egyben jogi keretét elsősorban az alábbi jogi rendelkezések jelentik:
a) a GDPR,
b) az Alaptörvény,
c) az Infotv.,
d) a nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény (a továbbiakban: Nftv.)
e) a nemzeti köznevelésről szóló 2011. évi CXC. törvény (a továbbiakban: Nknt.)
f) a felnőttképzésről szóló 2013. évi LXXVII. törvény (a továbbiakban: Fktv.)
g) az egészségügyről szóló 1997. évi CLIV. törvény (a továbbiakban: Eütv.),
h) az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény (a továbbiakban: Eüak.),
i) a munka törvénykönyvéről szóló 2012. évi I. törvény (a továbbiakban: Mt.),
j) a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény (a továbbiakban: Ltv.),
k) a Polgári Törvénykönyvről szóló 2013. évi V. törvény (a továbbiakban: Ptk.)
l) a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény (a továbbiakban: SzVMt.).
(2) A különböző állami irányító szervezetek, felügyeleti szervek és hatóságok által kibocsátott, kötelező érvényű adatvédelmi tárgyú állásfoglalást, véleményezést, iránymutatást, döntést minden adatkezelést végző szervezeti egységnek a lehető legrövidebb időn belül adaptálnia kell a hozzá tartozó munkafolyamataiba, továbbá amennyiben szükséges, be kell építeni az Egyetem Adatvédelmi Rendjébe.
(3) Az Egyetem, az adatvédelmi tisztviselő előzetes jóváhagyásával, valamennyi személyes adat kezelése során figyelembe veszi a különböző állami irányító szervezetek, felügyeleti szervek és hatóságok által kibocsátott, nem kötelező érvényű adatvédelmi tárgyú állásfoglalásokat, iránymutatásokat, szakmai véleményeket és ajánlásokat is, mindaddig, amíg ezek érvénytelenségét bíróság vagy hatóság meg nem állapítja.
(4) A (2) és a (3) bekezdésben rögzített állásfoglalásokról, véleményekről, iránymutatásokról, ajánlásokról a JII vezetője nyilvántartást vezet. A szervezeti egységek vezetői kötelesek a hozzájuk beérkező ilyen típusú dokumentum másolati példányát megküldeni a JII-nek.

### *A Szabályzat és az Egyetem belső szabályzatai közti koherencia*

5. §

*[Kapcsolódó jogi háttér: GDPR (78) preambulumbekezdése]*

(1) A Szabályzat, a hatálya alá tartozó minden adatkezelés vonatkozásában, az Egyetem más releváns szabályzatainak általános kereteként értelmezendő, így az azokban lévő adatkezeléseket e Szabályzat előírásai mentén kell értelmezni és végrehajtani.
(2) A Szabályzat hiteles módú értelmezését kizárólag a DPO végezheti.
(3) A Szabályzat szorosan összekapcsolódik különösen
a) az Egyetem Szervezeti és Működési Rendjével (a továbbiakban: SZMr),
b) az Egyetem Informatikai Biztonsági Szabályzatával, valamint
c) az Egyetem Iratkezelési Szabályzatával,
d) az Egyetem Tanulmányi és Vizsgaszabályzatával.
(4) Az Egyetem újonnan létrejövő, személyes adatkezelést érintő belső szabályozói jelen Szabályzat előírásainak figyelembevételével jöhetnek létre. A belső szabályozó elfogadása előtt a DPO szakmai véleményét minden esetben szükséges kikérni. A szakmai véleményezésre legalább 7 munkanapot szükséges biztosítani a DPO számára.
(5) Az Egyetem már hatályban lévő, személyes adatkezelést érintő módosuló belső szabályozói kapcsán a Szabályzat jelen szakasz (4) bekezdésében rögzített eljárás érvényes.
(6) Amennyiben a (3) bekezdés a)-e) pontjai szerinti valamely belső szabályozó ellentétesnek bizonyulna a Szabályzat valamely rendelkezésével, a DPO ennek észlelését követően haladéktalanul köteles erre a körülményre egyidejűleg a Kancellár, a Főtitkár és a JII vezetője figyelmét felhívni.
(7) Amennyiben a (3) bekezdés a)-e) pontjában nem említett valamely további belső szabályozó ellentétesnek bizonyulna a Szabályzat valamely rendelkezésével, a DPO ennek észlelését követően haladéktalanul köteles erre a körülményre egyidejűleg a Kancellár, a Főtitkár és a JII vezetője figyelmét felhívni.
(8) Az Egyetem bármelyik munkavállalója, érintettje, adatkezelésben érintett partnere jelezheti a DPO felé, ha az Egyetem valamely belső szabályzója ellentétes jelen Szabályzatban előírtakkal. A DPO ezt a jelzést kivizsgálja, és amennyiben a jelzés jogos, akkor a (6) és (7) bekezdésekben leírtak alapján köteles eljárni.
(9) A (6) és (7) bekezdésben leírtak szerinti DPO jelzést követően a Szabályzattal ellentétes belső szabályzó alapján a továbbiakban adatkezelés nem folytatható. A JII a DPO jelzését követően köteles erről tájékoztatni a kérdéses adatkezeléssel érintett valamennyi szervezeti egységet, és mielőbb köteles a DPO jelzés alapján az érintett belső szabályzót felülvizsgálni és jelen Szabályzattal való összhangját megteremteni.

### **A Szabályzat célja**

6. §

*[Kapcsolódó jogi háttér: GDPR 5. cikk (2) bekezdése]*

Jelen Szabályzat célja, hogy az Egyetem, elsősorban, mint adatkezelő által, másodsorban, mint adatfeldolgozó által végzett adatkezelési tevékenység kapcsán
a) biztosítsa a természetes személyek számára a személyes adataik védelmével kapcsolatos jogokat, az emberi méltóságuk tiszteletben tartását, az információs önrendelkezés lehetőségét, és

b) hatékony belső védelmi mechanizmust hozzon létre az illetéktelen adatkezelések megakadályozására, hogy maradéktalanul megfeleljen a jogszabályi előírásoknak, figyelemmel az Egyetem SZMr-jére és a társadalmilag jelentős feladatellátásra, valamint
c) biztosítsa a személyes adatok kezelésének átláthatóságát és szabályozott keretek között történő, jogszerű megvalósulását.

## A Szabályzat fogalmi rendszere

7. §

*[Kapcsolódó jogi háttér: GDPR 4. cikk, valamint Infotv. 3. § 3. pontja, 11-13. pontjai, 16-17. pontjai, 21. pontja, 23-24. pontjai]*
*[Kapcsolódó háttéranyag: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_hu.pdf]*

Jelen Szabályzat alkalmazásában az alábbi fogalmakat szükséges irányadónak tekinteni:

1. ***adatállomány:*** egy adott nyilvántartási rendszerben kezelt adatok összessége.

2. ***adatfeldolgozó:*** az adatkezelő személyétől elkülönülő olyan természetes vagy jogi személy vagy bármely egyéb jogalany, aki adatfeldolgozói szerződés alapján – beleértve a jogszabály rendelkezése alapján kötött szerződést is – személyes adatok feldolgozását végzi az adatkezelő nevében, érdekében.

3. ***adatfeldolgozás:*** az adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által kifejtett, személyes adathoz vagy adatállományhoz kapcsolódó bármilyen adatkezelési feladatának elvégzése, függetlenül e feladatának végrehajtásához alkalmazott módszertől és eszköztől, valamint azok helyétől, annak időtartamától.

4. ***adatkezelés:*** a személyes adaton vagy adatállományon, automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége. Így különösen a gyűjtést, rögzítést, rendszerezést, tagolást, tárolást, átalakítást vagy megváltoztatást, lekérdezést, betekintést (megtekintést), felhasználást, közlést (ideértve a továbbítással történő közzétételt is), terjesztést vagy egyéb módon történő hozzáférhetővé tételt, összehangolást vagy összekapcsolást, korlátozást, törlést, illetve megsemmisítést, valamint a személyes adat további felhasználásának, nyomon követhetőségének megakadályozását.

5. ***adatkezelés korlátozása:*** a tárolt személyes adat vagy adatállomány megjelölése egy meghatározott ideig fennálló jövőbeli kezelésük korlátozása céljából (zárolás). Az így megjelölt személyes adaton, vagy adatállományon a tárolás kivételével adatkezelési műveletet nem lehet végrehajtani a korlátozás feloldásáig.

6. ***adatkezelő:*** az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza, illetve a vonatkozó döntéseket meghozza, valamint végrehajtja, vagy adatfeldolgozóval végrehajtatja.

*7.* ***adatkezelést végző szervezeti egység:*** az Egyetem SZMr-je által felhatalmazott feladatellátás során személyes adatot kezelő, kötelezettség-vállalásra jogosult szervezeti egység, függetlenül attól, hogy adatkezelői vagy adatfeldolgozói pozícióban végzi az adatkezelést. Két típusát különböztetjük meg az Egyetemen, úgymint
a) központi adatkezelést végző szervezeti egységek: az Egyetem SZMr-je értelmében a Rektori-Kancellári Kabinet, az Egyetem valamennyi gazdálkodásirányítási és igazgatási egysége, valamint az Egyetem valamennyi központi szolgáltató egysége, továbbá az Egyetem oktatási és tudományos kutatási szervezeti egységei közül valamennyi kar, a Klinikai Központ, az SZTE Bajai Obszervatóriuma, valamint az Interdiszciplináris Kutatásfejlesztési és Innovációs Kiválósági Központ.
b) helyi adatkezelést végző szervezeti egységek: az Egyetem központi adatkezelést végző szervezeti egységének nem minősülő szervezeti egységek.
Ahol a Szabályzat adatkezelést végző szervezeti egység megnevezést használja, azon – hatáskörre, valamint a hatékony feladatellátás megszervezésének elvárására, továbbá az együttműködési kötelezettség elvének figyelembevételével – mind a központi és mind a helyi adatkezelést végző szervezeti egységet érteni kell.

8. ***adatmegsemmisítés:*** a személyes adatot vagy adatállományt tartalmazó papíralapú, vagy elektronikus adathordozó teljes és végérvényes fizikai megsemmisítése (felszámolása, felülírása).

9. ***adattovábbítás:*** az adat meghatározott harmadik fél számára történő hozzáférhetővé tétele, ideértve az adatokba történő betekintés vagy kivonat készítés lehetővé tételét is.
Nem minősül adattovábbításnak:

a) az Egyetem szervezeti rendszerén belüli adatátadás munkamegosztás okán,
b) a személyes adatok adatfeldolgozó részére történő átadása,
c) az érintett saját személyes adataihoz való hozzáférésének biztosítása.

10. ***adattörlés:*** a személyes adat vagy adatállomány felismerhetetlenné tétele olyan módon, hogy a helyreállítása többé nem lehetséges, ideértve az Egyetem által jogszerűen kezelt személyes adat vagy adatállomány anonimizálását is.

11. ***Adatvédelmi Hatóság:*** a magyar jog által kijelölt adatvédelmi felügyeleti hatóság (jelenleg Nemzeti Adatvédelmi és Információszabadság Hatóság, NAIH).

12. ***adatvédelmi incidens:*** a személyes adatok kezelésénél megkövetelt adatbiztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi vagy eredményezheti.

13. ***adatvédelmi integritássértés:*** minden olyan akár intézkedésben, akár döntésben, akár eljárásban megvalósuló cselekmény vagy mulasztás, amely magába foglalja mind az adatvédelmi jogi előírásoknak, mind az Egyetem Adatvédelmi Rendjében leírtaknak, valamint az Egyetem felsővezetése által kitűzött adatvédelmi célkitűzéseknek, értékeknek és elveknek megfelelő működés sérelmét, vagy ilyen sérelem bekövetkezésével fenyeget.

14. ***adatvédelmi közérdekű bejelentés:*** olyan kérelem, amelyben a közérdekű bejelentő egy adott adatvédelmi integritássértés orvoslására, megszüntetésre hívja fel a figyelmet az adatkezelőhöz tartozó érintettek vagy azok bizonyos csoportja érdekeinek védelmében.

15. ***adatvédelmi panasz:*** olyan kérelem, amely egyéni adatvédelmi jog-, vagy érdeksérelem megszüntetésére irányul.

16. ***Adatvédelmi Rend:*** az Egyetem belső adatvédelmi szabályozóinak gyűjtő megnevezése.
17. ***anonim adat:*** minden olyan adat anonimnak minősül, amely alapján az érintett személyét sem az adatkezelő, sem más személy, szervezet nem, vagy többé már (visszafordíthatatlan módon) nem tudja azonosítani az egyén azonosítására észszerűen feltételezhetően alkalmas módszerrel.

18. ***álnevesítés:*** a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve, hogy
- az álnevesített személyes adat az eredeti személyes adattól, továbbá a kiegészítő információtól külön kerül tárolásra, valamint
- technikai és szervezési intézkedések megtételével biztosított egyfelől, hogy az álnevesített személyes adatokat kezelő személy az álnevesített személyes adatot nem tudja hozzákapcsolni azonosítási céllal az érintetthez, másfelől, hogy az álnevesített személyes adatok feloldása szigorú rend szerint csak az arra kijelölt személyek számára lehetséges csupán.

19. ***biometrikus adat:*** egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adata, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat.

20. ***címzett:*** bármely természetes vagy jogi személy, aki vagy amely számára személyes adatot az adatkezelő, illetve az adatfeldolgozó jogszerűen közöl. Azon közhatalmi szervek, amelyek egy egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnek.

21. ***egészségügyi adat:*** egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adata, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról.

22. ***érintett:*** bármely információ alapján azonosított vagy azonosítható természetes személy. Így minden természetes személy – függetlenül attól, hogy az Egyetemmel milyen jogviszonyban vagy kapcsolatban áll – saját személyes adatai vonatkozásában érintettnek minősül.

23. ***érintett hozzájárulása:*** az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez.

24. ***genetikai adat:*** egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az említett természetes személyből vett biológiai minta elemzéséből ered.

25. ***harmadik ország:*** minden olyan állam, amely
- nem az Európai Unió tagállama, illetve nem az Európai Gazdasági Térségről szóló megállapodásban részes állam, és
- amelynek állampolgára nemzetközi szerződés alapján nem élvez azonos jogállást az Európai Unió, illetve az EGT-állam állampolgárával.

26. ***harmadik fél:*** olyan természetes vagy jogi személy, aki vagy amely nem azonos
- az érintett személlyel,
- az adatkezelővel vagy az adatfeldolgozóval (ide értve a konkrét adatkezelést végző személyi állományukat is).

27. ***különleges adat:*** a személyes adatok különleges kategóriájába tartozik minden személyes adat, amely a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utal, valamint genetikai adatnak, a természetes személyek egyedi azonosítását célzó biometrikus adatnak, egészségügyi adatnak és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatnak minősül.

28. ***megismerhetővé tétel:*** a személyes adatok bármilyen módon megvalósuló – ideértve a szóbeli vagy írásbeli közlést, ráutaló magatartással, illetve mulasztással beálló hozzáférhetővé tételt, nyilvánosságra hozatalt – átadása, továbbítása.

29. ***nemzetközi szervezet:*** a nemzetközi közjog hatálya alá tartozó szervezet vagy annak alárendelt szervei vagy olyan egyéb szerv, amelyet két vagy több ország közötti megállapodás hozott létre, vagy amely ilyen megállapodás alapján jött létre.

30. ***nyilvánosságra hozatal:*** az adat bárki számára történő hozzáférhetővé tétele.

31. ***nyilvántartási rendszer:*** a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint – tagolt adatállománya, amely meghatározott ismérvek alapján hozzáférhető, függetlenül a nyilvántartási rendszer adathordozójától.

32. ***profilalkotás:*** a személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők – különösen a munkahelyi teljesítmény, a gazdasági helyzet, az egészségi állapot, a személyes preferenciák, az érdeklődés, a megbízhatóság, a viselkedés, a tartózkodási hely vagy a mozgáshoz kapcsolódó jellemzők – elemzéséhez, kiértékeléséhez vagy előrejelzéséhez használják fel.

33. ***személyes adat:*** a természetes személyre („érintett”) vonatkozó bármely információ, függetlenül attól, hogy az Egyetem adatkezelőként vagy adatfeldolgozói minőségében kezeli azt, illetve, hogy az adatkezelés teljesen vagy részben automatizált módon, informatikai eszközzel vagy manuális módon, papíralapon, továbbá, hogy a személyes adat kezelése adatállományban vagy azon kívül történik. Személyes adatnak minősül például a név, a személyazonosításra szolgáló bármely okmány adatköre, a helymeghatározó adat, az online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező vagy a társadalombiztosítási azonosító jel, az adóazonosító jel, a születési adatok, a lakóhely, a tartózkodási hely, az e-mail cím, a telefonszám, a GPS-koordináta, az IP-cím, a MAC-cím,

az önéletrajzi adat, a személyiségi teszt eredménye, a saját vélemény, a fénykép, a videófelvétel, a hangfelvétel, a vizsgateljesítmény és az érdemjegy is.

34. ***tiltakozás:*** az érintett nyilatkozata, amellyel személyes adatának kezelését kifogásolja, vitatja és az adatkezelés megszüntetését, illetve a kezelt adat törlését kéri.

## Az Egyetem Adatvédelmi Rendje

8. §

*[Kapcsolódó jogi háttér: GDPR 24. cikk (1)-(2) bekezdései, valamint (77)-(78) preambulumbekezdései]*

(1) Az Egyetem feladatellátása során kezelt személyes adat adatkezelésének előírásait az Egyetem Adatvédelmi Rendje szabályozza.
(2) Az Egyetem Adatvédelmi Rendje gyűjtőelnevezése az Egyetem valamennyi belső, adatvédelmi tárgykörű szabályozóinak, amely a (3) bekezdésben rögzítetteket foglalja magába.
(3) Az Egyetem Adatvédelmi Rendjébe tartozik:
a) jelen Szabályzat,
b) az Egyetem Adatvédelmi Eljárásrendje,
c) az Egyetem Egészségügyi Adatkezelési Eljárásrendje,
d) az Egyetem Köznevelési Adatkezelési Eljárásrendje,
e) az Egyetem speciális adatkezelési tárgykörökre vonatkozó adatkezelési eljárásrendjei,
f) a DPO iránymutatások.
(4) Az elfogadott Egyetem Adatvédelmi Rend elemeiről a JII nyilvántartást vezet, valamint kihirdeti és közzéteszi azokat az egyetemi polgárok számára.
(5) A DPO iránymutatások a 13. § (2) bekezdésében leírtak szerint kerülnek kihirdetésre.

## *Az Egyetem Adatvédelmi Szabályzata és Eljárásrendje*

9. §

(1) A 8. §-ban részletezett Adatvédelmi Rend átalános keretét jelen Szabályzat alkotja.
(2) A Szabályzat elkészítése és naprakészen tartása a JII feladata.
(3) A Szabályzat elfogadása és módosítása, a DPO szakmai véleményének kikérését követően, a Szenátus hatáskörébe tartozik.
(4) A Szabályzathoz Adatvédelmi Eljárásrend készülhet az Egyetem egészére nézve, amelynek célja a Szabályzat rendelkezéseinek a napi gyakorlatban történő megvalósítása. Az Adatvédelmi Eljárásrend elkészítésének szükségességére a DPO tesz javaslatot az Egyetem adatkezelési gyakorlatának függvényében a Kancellár és a JII vezetője felé. Az Adatvédelmi Eljárásrendet a JII állítja össze, és annak elfogadása, a DPO szakmai véleményének kikérését követően, a Kancellár hatáskörébe tartozik. Az Adatvédelmi Eljárásrend belső használatra készül.

### *Az Egyetem Egészségügyi Adatkezelési Eljárásrendje*

10. §

(1) Az Egyetem Egészségügyi Adatkezelési Eljárásrendjének elkészítése és naprakészen tartása a KK elnökének, valamint a JII feladata.
(2) Az Eljárásrend elfogadása és módosítása, a DPO szakmai véleményének kikérését követően, a Szenátus hatáskörébe tartozik.

### *Az Egyetem Köznevelési Adatkezelési Eljárásrendje*

11. §

(1) Az Egyetem Köznevelési Adatkezelési Eljárásrendjének elkészítésére az Egyetem bármelyik köznevelési intézménye javaslattal élhet a JII felé.
(2) Az Eljárásrend elkészítése és naprakészen tartása a JII feladata. Az Egyetem köznevelési intézményei vezetőinek bevonása az Eljárásrend véglegesítési munkafolyamatába, valamint az Eljárásrend elfogadásának koordinációja a JII feladata.
(3) Az Eljárásrend elfogadása és módosítása, a DPO szakmai véleményének kikérését követően, a Szenátus hatáskörébe tartozik.
(4) Ameddig a köznevelési intézmények ilyen kezdeményezéssel nem élnek, addig az Nknt. 43. § (1) bekezdés alapján rögzített adatkezelési szabályzat alatt az Egyetem Adatvédelmi Szabályzatát, valamint Adatvédelmi Eljárásrendjét szükséges érteni.

### *Speciális adatkezelések eljárásrendjei*

12. §

(1) Az Egyetemen megvalósuló speciális adatkezelésekre jelen Szabályzat általános szabályait irányadónak kell tekinteni.
(2) A Kancellár az Egyetem speciális adatkezelési tárgyköreire nézve speciális adatvédelmi előírásokat fogalmaz meg jelen Szabályzat kiegészítéseként.
(3) Speciális adatkezelésnek minősülnek különösen az alábbi témakörök:
a) a kamerás adatkezelés
b) a telefonbeszélgetések rögzítése
c) az elektronikus levelezések, valamint hírlevelezés
d) az Egyetem egységei által létrehozott közösségi oldalak, médiaplatformok használata
e) a munkahelyi adatkezelések (különös figyelemmel az álláshirdetéshez, felvételhez, munkáltatói ellenőrzésekhez, valamint a munkaviszony megszűnéséhez kapcsolódó adatvédelmi előírások).
(4) A DPO feladata, hogy az adott speciális adatkezelésekhez tartozó adatkezelési eljárásrend elfogadásának szükségességére javaslatot tegyen. Ezen javaslatát a Kancellár és a JII felé elektronikus úton teszi meg.
(5) A (4) bekezdésben részletezett DPO javaslat elfogadásáról szóló döntésről való tájékoztatást követően a speciális adatkezelési eljárásrend előkészítése a JII feladata.

(6) Bármelyik egyetemi polgár javaslatot tehet a DPO felé speciális adatkezelési eljárásrend elfogadására. A DPO köteles a javaslatot érdemben megvizsgálni az adatvédelmi jogi előírások és az Adatvédelmi Rend figyelembe vételével. Amennyiben a javaslat jogos, a DPO jelen szakasz (4) bekezdésében leírtak szerint jár el.
(7) A JII feladata a speciális adatkezelések vonatkozásában az adatkezelési eljárásrendek véglegesítése, elfogadásuk, kihirdetésük koordinálása, és azok naprakészen tartása a (8) bekezdésben leírt elfogadást követően.
(8) A speciális adatkezelési eljárásrend elfogadása és módosítása, a DPO szakmai véleményének kikérését követően, a Kancellár hatáskörébe tartozik.

### *DPO iránymutatások*

13. §

(1) A DPO megkeresés alapján vagy hivatalból, komplex adatkezelési ügyekben, saját hatáskörében eljárva iránymutatást készít (ún. DPO iránymutatás).
(2) A DPO az elkészített iránymutatást megküldi a JII felé. A JII a tárgykörrel érintett egység adatvédelmi referensei számára kihirdeti azt, akik gondoskodnak a DPO iránymutatásban foglaltak eljuttatásáról az egység vezetője és – a vezető döntésének megfelelő módon – a munkatársak felé.
(3) A DPO iránymutatásokról a JII nyilvántartást vezet.
(4) A DPO elfogadott iránymutatásait rendszeresen, legalább 3 évente, felülvizsgálja. Amennyiben szükséges javaslatot tesz az Adatvédelmi Rend módosítására, kiegészítésére. Erre vonatkozó javaslatát a Kancellár és a JII felé elektronikus levélben teszi meg.

## Alapelvek

14. §

*[Kapcsolódó jogi háttér: GDPR 5. cikke, valamint a GDPR 83. cikk (5) bekezdés a) pontja, Infotv. 61. § (4) bekezdés]*

(1) Már az adatfelvétel megtervezésekor és az adatkezelés bármelyik szakaszában ügyelni kell a személyes adatok felvételének és kezelésének jogszerűségére, a személyes adatok pontosságának biztosítására, a feladatellátáshoz szükséges és még éppen elégséges mértékű teljességére, időszerűségére, azok megfelelő időtartamú és biztonságos tárolására, hogy emiatt az érintettek jogai ne sérülhessenek.
(2) Az adatkezelések kapcsán az alábbi elveket betartva szükséges eljárni, úgymint
a) a jogszerűség, a tisztességes eljárás és az átláthatóság elve
b) a célhoz kötöttség elve
c) a pontosság elve
d) a korlátozott tárolhatóság elve
e) az adattakarékosság elve
f) az integritás és bizalmasság elve
g) az elszámoltathatóság elve.

(3) Az alapelvsérelem a legmagasabb bírságolás lehetőségét vonja maga után, ennek okán különös figyelemmel kell eljárni az adatkezelési folyamatok minden szakaszában (tervezés, megvalósítás, ellenőrzés), hogy az adatvédelmi alapelvek a lehető legteljesebb mértékben érvényesülhessenek.
(4) Bármely egyetemi polgárnak jogában áll a hatáskörébe tartozó adatkezelés bármelyik szakaszában közvetlenül tanácsot kérni a DPO-tól az alapelvek jogszerű érvényesíthetősége kapcsán.

### *Jogszerűség, a tisztességes eljárás és az átláthatóság alapelve*

15. §

*[Kapcsolódó jogi háttér: GDPR (39)-(40), (58), (60) preambulumbekezdései, 5. cikk (1) bekezdés a) pontja]*

(1) A jogszerűség, a tisztességes eljárás és az átláthatóság alapelve értelmében a személyes adatok kezelését jogszerűen, tisztességesen, valamint az érintett számára átlátható módon kell végezni.
(2) Jogszerű az adatkezelés, ha a mindenkor hatályos adatvédelmi szabályozásoknak megfelel, ideértve az Egyetem Adatvédelmi Rendjét is.
(3) Tisztességes az adatkezelés, ha az adatkezelés érintettjeinek jogait (ideértve az emberi méltóságot is) tiszteletben tartva tervezik és valósítják meg.
(4) Átlátható az adatkezelés, ha az adatkezelést az érintett megismerheti, az érintetti sajátosságokra (különösen életkor, belátási képesség) is figyelemmel értelmezheti azt, és nyomon követheti az adatkezelési folyamatot. Az átláthatóság alapelvének garanciái különösen az adatkezelési tájékoztató elkészítése és közzététele az érintettek számára, a személyes adatokhoz való hozzáféréshez és másolathoz való érintetti jog biztosítása, valamint az adatkezelési tevékenységek nyilvántartásának vezetése is.

### *Célhoz kötöttség alapelve*

16. §

*[Kapcsolódó jogi háttér: GDPR (39) preambulumbekezdése, 5. cikk (1) bekezdés b) pontja]*

(1) A célhoz kötöttség elve értelmében személyes adat gyűjtése és kezelése csak meghatározott, egyértelmű és jogszerű célból történhet.
(2) A készletező, úgynevezett jövőbeli eshetőleges felhasználásra szolgáló adatgyűjtés tilos.
(3) Személyes adatot a jogszerű működéssel összefüggésben felmerült célokból, így különösen a felsőoktatási tevékenység (oktatás, tudományos kutatás és művészeti alkotótevékenység, konferencia-szervezés) ellátása céljából, foglalkoztatási célból, marketing (toborzás) és közvetlen üzletszerzés (direktmarketing) céljából, kollégiumok üzemeltetése, személy- és vagyonbiztonságot szolgáló eszközök üzemeltetése céljából, az egyetemi működéshez kapcsolódó iratkezelési folyamatok, informatikai szolgáltatások, az információbiztonság biztosítása céljából, könyvtári, levéltári és nyelvvizsga szolgáltatás céljából, az egészségügyi szolgáltatások nyújtása, valamint az Egyetem Alapító Okiratában meghatározott további alaptevékenységek ellátása céljából kerülhet sor.

(4) Az Egyetem tanulmányi rendszerében az intézmény rendeltetésszerű működéséhez, a jelentkezők és a hallgatók jogainak gyakorlásához és kötelezettségeinek teljesítéséhez, a képzés, kutatás megszervezéséhez, a munkáltatói jogok gyakorlásához, illetve az oktatók, kutatók, dolgozók jogainak gyakorlásához és kötelezettségeik teljesítéséhez, a jogszabályokban meghatározott nyilvántartások vezetéséhez, a jogszabályokban és a felsőoktatási intézmény szervezeti és működési szabályzatában biztosított kedvezményekre való jogosultság megállapításához, elbírálásához és igazolásához, a végzettek pályakövetése céljából nélkülözhetetlenül szükséges személyes és különleges adatokat tartja nyilván.
(5) Az Egyetem egészségügyi informatikai rendszerében a KK közfeladatának ellátása érdekében a jelentkező betegek gyógykezelése, állapotuk nyomon követése, a beteg- és orvosjogok érvényesítése, a társadalombiztosítás terhére biztosított ellátások elszámolása, különböző alkalmassági vizsgálatok véleményezése, a KK ellátási folyamatainak minőségbiztosítása, egészségügyi igazolások és javaslatok készítése, orvos-szakmai képzések, továbbképzések, valamint tudományos kutatás, továbbá jogszabályban előírt további kötelezettségek teljesítése céljából elengedhetetlenül szükséges egészségügyi adatokat tartja nyilván.
(6) A személyes adatok célhoz kötöttségének elve értelmében az egyes eljárások során kezelt személyes adatokat csak az adott jogszerű ügymenet elintézése érdekében szabad felhasználni, más eljárásokkal**,** illetve adatokkal azok nem kapcsolhatók össze, az adatgyűjtés céljától eltérő célból nem kezelhetők– kivéve, ha
a) ezt a GDPR 23. cikk (1) bekezdésében rögzített célok eléréséhez szükséges intézkedésnek minősülő uniós vagy magyar jogszabály törvény rendeli el, vagy
b) az érintett önkéntesen hozzájárult és az adatkezelés feltételei minden egyes személyes adatára vonatkozóan fennállnak, vagy
c) az adatkezelést végző szervezeti egységek vezetői az indokok pontos megjelölésével kérelmet terjesztenek elő a DPO-nál. A DPO a kérelmet szakmailag véleményezi, majd a kérelmet, szakmai véleményével együttesen, megküldi a Kancellár és a JII felé döntés meghozatala céljából.
(7) A (6) bekezdésben leírtak tekintetében annak megállapításához, hogy az eltérő célú adatkezelés összeegyeztethető-e azzal a céllal, amelyből a személyes adatokat eredetileg gyűjtötték, figyelembe kell venni többek között
a) a személyes adatok gyűjtésének céljait és a tervezett további adatkezelés céljai közötti esetleges kapcsolatokat;
b) a személyes adatok gyűjtésének körülményeit, különös tekintettel az érintettek és az adatkezelő közötti kapcsolatokra;
c) a személyes adatok jellegét, különösen pedig azt, hogy különleges személyes adatok kezeléséről van-e szó, illetve, hogy büntetőjogi felelősség megállapítására és bűncselekményekre vonatkozó adatoknak a kezeléséről van-e szó;
d) azt, hogy az érintettekre nézve milyen esetleges következményekkel járna az adatok tervezett további kezelése;
e) megfelelő garanciák meglétét, ami jelenthet titkosítást vagy álnevesítést is.

### *Pontosság alapelve*

17. §

*[Kapcsolódó jogi háttér: GDPR 5. cikk (1) bekezdés d) pontja]*

(1) A pontosság elve értelmében a személyes adatoknak az adatkezelési cél megvalósítása érdekében és azzal összefüggésben pontosnak, naprakésznek és teljeskörűnek kell lenniük.

(2) Minden észszerű intézkedést meg kell tennie az adatkezelést végző szervezeti egység vezetőjének, hogy az adatkezelés célja szempontjából pontatlan személyes adatokat az adatkezelést végző személy haladéktalanul képes legyen helyesbíteni, az adatkezelés célja szempontjából szükségtelen, vagy a valóságnak nem megfelelő adatokat pedig haladéktalanul törölni.

***Korlátozott tárolhatóság alapelve***

18. §

*[Kapcsolódó jogi háttér: GDPR (39) preambulumbekezdése, 5. cikk (1) bekezdés e) pontja és az Infotv. 5. § (5) bekezdés]*

(1) A korlátozott tárolhatóság elve értelmében a személyes adatok tárolásának olyan módon kell megtörténnie, amely az érintettek azonosítását csak az adott adatkezelési cél eléréséhez szükséges ideig teszi lehetővé.
(2) A személyes adatok megőrzési idejét minden esetben az adott adatkezelés célja határozza meg.
(3) A célhoz nem kötött és olyan személyes adatokat, amelyekre nézve az adatkezelés célja megszűnt vagy szűkítő jelleggel módosult, haladéktalanul, illetve a célhoz igazodóan előírt megőrzési határidő leteltével meg kell semmisíteni, kivéve, ha az érintett személy a korlátozáshoz való jogát gyakorolja. Ezen kötelezettség a személyes adat adathordozójától független követelmény.
(4) A személyes adatokat tartalmazó iratanyagok megsemmisítéséről a szükséges biztonsági intézkedések mellett kell gondoskodni az Egyetem Iratkezelési Szabályzatnak megfelelően.
(5) Amennyiben jogi előírás nincs az adatkezelés időtartamára nézve vagy nincs szükség annak időszakos felülvizsgálatára, és az adatkezelés célja folyamatos jellegű, akkor az ilyen jellegű adatkezeléseket legalább 3 évente felül kell vizsgálnia az adatkezelést végző szervezeti egységnek. A felülvizsgálatot és annak eredményét dokumentálni kell, és a felülvizsgálat elvégzését követő 10 évig kötelező azt megőrizni. Ezen dokumentációt az Adatvédelmi Hatóság eljárása során ellenőrzi.
(6) Az önkéntes hozzájárulás alapján visszavonásig kezelt személyes adatok vonatkozásában az adatkezelés célját legalább 10 évente szükséges dokumentáltan felülvizsgálnia az adatkezelést végző szervezeti egységnek. A felülvizsgálati dokumentálásra az (5) bekezdésben leírtak alkalmazhatók.
(7) A személyes adatoknak az előre meghatározott megőrzési időn túli további őrzése történelmi vagy tudományos kutatás céljából a GDPR 89. cikk alapján lehetséges. Erre való igényt az Egyetem kutatói a törlendő adatok lejáró megőrzési idejét megelőzően a DPO-nál terjeszthetnek elő. Pontosan meg kell határozniuk a tovább megőrzendő adatok körét, és meg kell indokolniuk a megőrzés szükségességét, figyelemmel jelen Szabályzatban írtakra, különösen az adatkezelés alapelveire. Az adatok törléséről vagy megtartásáról a Kancellár a DPO, egészségügyi adatok esetén a KK elnök, a DPO és az egészségügyi adatvédelmi tisztviselő véleményének figyelembe vételével határoz. Az adatokat a GDPR 89. cikke szerint véglegesen anonimizálni szükséges, ha ez nem lehetséges, akkor álnevesíteni kell. A kutatók az adatokhoz a kancellári, illetve KK elnöki jóváhagyás után juthatnak hozzá.

### *Adattakarékosság alapelve*

19. §

*[Kapcsolódó jogi háttér: GDPR (39) preambulumbekezdése, 5. cikk (1) bekezdés c) pontja]*

Az adattakarékosság alapelve értelmében az adatkezelés célja szempontjából szükséges és még éppen elégséges személyes adat kezelhető csupán.

### *Integritás és bizalmasság alapelve*

20. §

*[Kapcsolódó jogi háttér: GDPR 5. cikk (1) bekezdés f) pontja]*

(1) Az integritás és bizalmasság elve értelmében a személyes adatok kezelését oly módon kell végezni, hogy a mindenkori tudomány és technológia állása szerint megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, különösen az adatok jogellenes kezelésével, a véletlen elvesztéssel, a megsemmisítéssel vagy károsodással szemben.
(2) Az Egyetem vonatkozásában az adatbiztonság koordinálásáért az adatkezelést végző szervezeti egységektől szervezetileg elkülönülő, független információbiztonsági felelős felel. Az adatbiztonsági megfelelés érdekében tanácsadást, ellenőrzést, belső oktatást az információbiztonsági felelős végez.
(3) Az információbiztonsági felelős hatásköréről, jogállásáról az Egyetem Információbiztonsági Szabályzata rendelkezik, figyelemmel különösen jelen Szabályzat adatbiztonsági előírásaira, valamint az Egyetem Informatikai Biztonsági Szabályzatára.
(4) Az Egyetem Információbiztonsági Szabályzatának elkészítése és naprakészen tartása az Informatikai és Szolgáltatási Igazgatóság hatáskörébe tartozik, és annak elfogadása a Szenátus hatásköre.

### *Elszámoltathatóság alapelve*

21. §

*[Kapcsolódó jogi háttér: GDPR 5. cikk (2) bekezdés, valamint (82) preambulumbekezdés, valamint 30. cikk]*

(1) Az elszámoltathatóság elve értelmében jelen Szabályzat hatálya alá tartozó, személyes adatkezelést végző minden személy felelős a saját adatkezelési tevékenysége kapcsán az Adatvédelmi Rendben előírtaknak való megfelelésért, továbbá a hozzá tartozó adatkezelések teljes időtartama alatt bármikor képesnek kell lennie e megfelelés igazolására.
(2) A közvetlen munkáltatói jogkörrel rendelkező személy valamennyi beosztottja tekintetében a beosztottak munkaköri feladataikhoz tartozó adatkezelések kapcsán felelős, hogy
a) a beosztottja megismerje és megértse az Adatvédelmi Rendben leírtakat, és
b) a munkaköri feladatokba tartozó egyes adatkezelési tevékenységeket az Adatvédelmi Rend mentén az egyes beosztottjaival közösen átbeszélje, és

c) a beosztott személy munkaköri leírásába belekerüljenek az adott munkakörre szabott fontosabb adatvédelmi elvárások, és
d) a beosztott adatvédelmi tartalmú kérdését felelősen megválaszolja, vagy bizonytalanság esetén a központi szervezeti egységének vezetőjéhez forduljon tanácsért.
(3) Az elszámoltatható és átlátható adatkezelést segíti elő különösen
a) az adatkezelést végző szervezeti egységek adatkezelési tevékenységének nyilvántartása,
b) az Adatvédelmi Rendnek megfelelő nyilvántartási rendszer használata,
c) az egyedi adatátadás, valamint az egyedi adattovábbítás nyilvántartása,
d) az adatkezelési tájékoztatók elkészítése.

### *Jogalapok*

22. §

*[Kapcsolódó jogi háttér: GDPR 6. cikk, valamint 9. cikk]*

(1) Az adatkezelés abban az esetben jogszerű, ha a vonatkozó jogszabályoknak megfelelően az alábbi jogalapok legalább egyikén alapulóan történik, úgymint
a) az érintett önkéntes hozzájárulása (önkéntes hozzájáruláson alapuló jogalap),
b) az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az adatkezelés a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges (szerződéses jogalap),
c) az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges (jogi kötelezettség-teljesítésen alapuló jogalap),
d) az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges (létfontosságú érdeken alapuló jogalap),
e) az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges (közérdek jogalapja),
f) az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek (jogos érdeken alapuló jogalap).
(2) Kétség esetén, az adatkezelést végző személy írásos megkeresése esetén, a megfelelő jogalap kiválasztására a DPO tesz javaslatot. A megkeresést megfogalmazó munkatárs felel azért, hogy a jogalapot befolyásoló valamennyi adatkezelési körülményt feltárja a DPO előtt a jogalap pontos meghatározása érdekében.
(3) A különleges kategóriába tartozó személyes adatok kezelése alapvetően tilos. A jogszerű adatkezelés akkor valósulhat meg, ha az adatkezelésnek az (1) bekezdés szerinti jogalapja meghatározásra került, és a GDPR 9. cikk (2) bekezdésében felsorolt kivételek valamelyike teljesül, úgymint
a) jogszabály által nem tiltott esetkörben az érintett kifejezett hozzájárulását adta személyes adatai kezelésére;
b) az adatkezelés az adatkezelőnek vagy az érintettnek a foglalkoztatást, valamint a szociális biztonságot és szociális védelmet szabályozó jogi előírásokból fakadó kötelezettségei teljesítése és konkrét jogai gyakorlása érdekében szükséges, ha az érintett alapvető jogait és érdekeit védő megfelelő garanciákról is rendelkező uniós vagy tagállami jog, illetve a tagállami jog szerinti kollektív szerződés ezt lehetővé teszi;

c) az adatkezelés az érintett vagy más természetes személy létfontosságú érdekeinek védelméhez szükséges, ha az érintett fizikai vagy jogi cselekvőképtelensége folytán nem képes a hozzájárulását megadni;
d) az adatkezelés valamely politikai, világnézeti, vallási vagy szakszervezeti célú alapítvány, egyesület vagy bármely más nonprofit szervezet megfelelő garanciák mellett végzett jogszerű tevékenysége keretében történik, azzal a feltétellel, hogy az adatkezelés kizárólag az ilyen szerv jelenlegi vagy volt tagjaira vagy olyan személyekre vonatkozik, akik a szervezettel rendszeres kapcsolatban állnak a szervezet céljaihoz kapcsolódóan, és, hogy a személyes adatokat az érintettek hozzájárulása nélkül nem teszik hozzáférhetővé a szervezeten kívüli személyek számára;
e) az adatkezelés olyan személyes adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott;
f) az adatkezelés jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges, vagy amikor a bíróságok igazságszolgáltatási feladatkörükben járnak el;
g) az adatkezelés jelentős közérdek miatt szükséges, uniós jog vagy tagállami jog alapján, amely arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő;
h) az adatkezelés megelőző egészségügyi vagy munkahelyi egészségügyi célokból, a munkavállaló munkavégzési képességének felmérése, orvosi diagnózis felállítása, egészségügyi vagy szociális ellátás vagy kezelés nyújtása, illetve egészségügyi vagy szociális rendszerek és szolgáltatások irányítása érdekében szükséges, jogszabály alapján vagy egészségügyi szakemberrel kötött szerződés értelmében, továbbá, ha ezen adatok kezelése olyan személy által vagy olyan személy felelőssége mellett történik, aki jogszabályban meghatározott szakmai titoktartási kötelezettség hatálya alatt áll;
i) az adatkezelés a népegészségügy területét érintő olyan közérdekből szükséges, mint a határokon át terjedő súlyos egészségügyi veszélyekkel szembeni védelem vagy az egészségügyi ellátás, a gyógyszerek és az orvostechnikai eszközök magas színvonalának és biztonságának a biztosítása, és olyan uniós vagy tagállami jog alapján történik, amely megfelelő és konkrét intézkedésekről rendelkezik az érintett jogait és szabadságait védő garanciákra, és különösen a szakmai titoktartásra vonatkozóan;
j) az adatkezelés közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból szükséges olyan jogszabály alapján, amely arányos az elérni kívánt céllal, tiszteletben tartja a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő.

### *Önkéntes hozzájárulás*

23. §

*[Kapcsolódó jogi háttér: GDPR (32)-(33), valamint (42)-(43) preambulumbekezdések, 6. cikk (1) bekezdés a) pontja, valamint 7-8. cikkek]*

(1) Az érintett hozzájárulása akkor tekinthető az adott adatkezelés érvényes jogalapjának, ha
a) a hozzájárulás az érintett szabad akaratán alapul, és
b) bármilyen külső befolyástól, kényszertől, félelemtől, fenyegetéstől mentesen jön létre, kellő időt hagyva a megfontolt döntésre, és

c) megfelelő tájékoztatáson alapul, különösen jelen Szabályzat 34. § (1) bekezdésében, valamint 36. §-ában leírtakra figyelemmel, és
d) az érintett egyértelmű akaratnyilatkozatán alapulóan, félreérthetetlenül kifejezett cselekedet útján jön létre.
(2) A hallgatás, az előre bejelölt jelölőnégyzet (check-box) használata vagy a nem cselekvés nem minősül jogszerű hozzájárulásnak.
(3) Nem minősül jogszerűnek a hozzájárulás akkor sem, ha
a) a hozzájárulás körülményei, illetve következményei megakadályozzák az egyén valódi választási (döntési) szabadságát,
b) a hozzájárulás bárminemű közvetett vagy közvetlen befolyásoláson alapul,
c) egy adott szerződés teljesítését vagy egy adott szolgáltatás nyújtását olyan adatkezeléshez való hozzájáruláshoz kötik, amely nem szükséges a szerződés teljesítéséhez,
d) az érintett és az adatkezelő között egyértelműen egyenlőtlen (függő) viszony áll fenn – különösen a munkajogi alá- és fölérendeltségi, valamint az oktatói-hallgatói jogviszony esetén – és az adott adatkezelés a függő jogviszony keretében valósul meg, a függő jogviszonnyal összefügg. Ennek megfelelően az érintett hozzájárulása a munkaviszony és a hallgatói jogviszony kapcsán felmerülő adatkezelések tekintetében főszabály szerint nem lehet jogalap, a hozzájárulás csak kivételesen, olyan esetekben alapozhatja meg az adatkezelést, ha az adatkezelés semmilyen kapcsolatban nem áll a munkaviszonnyal, illetve a hallgatói jogviszonnyal (pl. a munkahelyi, ún. csapatépítő rendezvényen való részvétel esetén fénykép, illetve videofelvétel készítése, a rendezvénnyel összefüggésben az ételallergiára vonatkozó adatok kezelése, illetve az Egyetemet népszerűsítő, bemutatkozó anyagokban, kiadványokban történő szerepeltetéshez fénykép vagy videofelvétel készítése, továbbá egyetemi hallgató tudományos kutatás alanya akkor lehet önkéntes hozzájárulása alapján, ha a hallgató és a kutatást végző szervezeti egység között nem áll fenn függő viszony, azaz a szervezeti egység által oktatott tárgyakból a hallgató már eredményes vizsgát tett.)
(4) A hozzájárulás bármilyen formában megadható – papíralapon vagy elektronikusan.
a) A papíralapú hozzájárulást az érintett személy aláírásával hitelesíti.
b) Az elektronikus felületen keresztül megadott hozzájárulás – amennyiben az érintett azonosítható, a hozzájárulás ténye megfelelően rögzíthető és megőrizhető, illetve az érintett törlési kérelme esetén a vonatkozó személyes adatok törölhetők – megtehető:

- az Egyetem által nyilvántartott, az érintett által megjelölt, vagy amennyiben az érintett az Egyetemmel foglalkoztatási jogviszonyban áll, munkahelyi e-mail címéről küldött levélben, továbbá
- az Egyetemen általánosan használt oktatási (például Neptun, Modulo, CooSpace), pénzügyi (például Nexon) és betegellátási (kórház informatikai rendszerben), közérdekű információs (az Egyetem és a szervezeti egységei által működtetett hivatalos weboldal) rendszeren keresztül, ha az adatbiztonsági garanciák adottak, valamint
- az információbiztonságért felelős személy által előzetesen egyedileg vagy általánosságban jóváhagyott, e célra az adatkezelést végző szervezeti egység által létrehozott vagy kezdeményezett elektronikus űrlap segítségével.

(5) Az érintett hozzájárulásán alapuló adatkezelés esetén az adatkezelőnek az adatkezelés teljes időtartama alatt képesnek kell lennie annak igazolására, hogy az érintett személyes adatainak kezeléséhez hozzájárult.
(6) Hozzájáruláson alapuló adatkezelésnek minősülnek különösen az önkéntes feliratkozáson alapuló hírlevelek küldésével, nyereményjátékokban való részvétellel vagy különböző eseményekre való regisztrációval, kérdőívek kitöltésével, individualizált kép-és hangfelvétel készítésével vagy tudományos kutatásban való részvétellel összefüggő adatkezelési tevékenységek.

(7) Az adatkezelőnek biztosítania kell azt, hogy az érintett a hozzájárulását bármikor visszavonhassa, és e jogalapon kezelt személyes adatát töröltethesse, és a hozzájárulás visszavonását, vonatkozó személyes adataihoz kapcsolódó törlési jogának gyakorlását ugyanolyan egyszerű módon kell lehetővé tennie, mint annak megadását.
(8) Amennyiben a hozzájárulás visszavonása, az érintett törlési kérelme az adatkezelőt jogilag hátrányosan érintené, akkor az adatkezelés jogalapja eleve nem lehet önkéntes hozzájárulás.
(9) A hozzájárulást a különböző adatkezelési tevékenységekhez célonként külön-külön kell beszereznie az adatkezelőnek, valamint a hozzájárulás iránti kérelmet egyértelműen és világosan el kell választani az egyéb adatkezelési tevékenységektől vagy a szerződés többi részétől.
(10) Az adatkezelő köteles a hozzájárulás iránti kérelmet – a jogi előírások által megkövetelt elvárások mellett – közérthető módon és a lehető legegyszerűbb nyelvezettel megfogalmazni.
(11) Az önkéntes hozzájárulás megadását a 16 éven aluliak esetén a szülői felügyeletet gyakorló személy teheti meg. Az adott adatkezelést végző szervezeti egység, a kezelt adatok jellegére, és ezáltal a személyes adatok még hatékonyabb védelme érdekében, dönthet úgy, hogy ezt az életkori határt megemeli, viszont annak lecsökkentéséhez nincs joga. Az egészségügyi adatok kezelése során a 14. életévet betöltött személy véleményét az adatkezeléshez való hozzájárulás megadása és visszavonása kapcsán, a szakmailag lehetséges mértékig, figyelembe kell venni.
(12) Az érintett kérelmére, kezdeményezésére indult eljárásban vagy más ügyben az eljárás lefolytatásához az általa megadott személyes adatai kezeléséhez a hozzájárulását a kérelem, kezdeményezés leadásával megadottnak kell tekinteni, ha az adatkezelésnek nincsen más jogalapja.

### *Jogos érdek*

24. §

*[Kapcsolódó jogi háttér: GDPR (47) preambulumbekezdés, 6. cikk (1) bekezdés f) pontja]*

(1) A jogos érdek akkor teremthet jogalapot az adatkezelésre, ha az érintett érdekei, alapvető jogai és szabadságai nem élveznek elsőbbséget az adott adatkezelés tekintetében és nem kell jelen Szabályzat 25. §-a, illetve 28. §-a szerint eljárni.
(2) Jogos érdeken alapuló jogalap választása esetén az adatkezelést elrendelő, adatkezelést végző szervezeti egységnek érdekmérlegelési tesztet kell írásban készítenie az adatkezelési tájékoztató kihirdetése és a konkrét adatkezelési folyamat megkezdése előtt. Az érdekmérlegelés elvégzése nélkül a jogos érdek nem jogszerű adatkezelési jogalap.
(3) Az érdekmérlegelés tartalmazza legalább az alább felsorolt elemek mindegyikét:
a) az érdekmérlegelés tárgya,
b) az érdekmérlegelés elkészítésének időpontja (ez minden esetben előbbi dátum, mint az adatkezelés megkezdése, valamint az adatkezelési tájékoztatás megtörténte),
c) az érdekmérlegelést készítő neve, beosztása és aláírása,
d) az érdekmérlegelést jóváhagyó adatkezelést végző szervezeti egység vezetőjének neve, beosztása és aláírása,
e) adatkezelés célja,
f) annak elemzését, hogy van-e olyan megoldás, amely személyes adat kezelése nélkül alkalmas a tervezett célt elérni,
g) az adatkezelő jogos érdekeinek felsorolása,

h) azon érintetti jogok, szabadságok felsorolása, amelyet érint a tervezett adatkezelés,
i) annak kiértékelése, hogy az adatkezelő érdekeinek és az érintettek jogainak korlátozása arányos és szükséges-e a tervezett adatkezelési céllal,
j) annak leírása, hogy milyen garanciák kerülnek beépítésre a folyamatba az érintetti jogok védelme érdekében.
(4) Az érdekmérlegelés elkészítésébe a DPO az adatkezelést végző szervezeti egység vezetőjének megkeresésére tanácsadóként bevonható. Az érdekmérlegelési teszt elkészítéséhez operatív segítség kérhető a JII-tól.
(5) Az elkészített érdekmérlegeléseket a központi adatkezelést végző szervezeti egység adatvédelmi referense tartja nyilván, és az érintett személyt tájékoztatja az elvégzett érdekmérlegelés eredményéről, amennyiben az érintett ezt írásban (ideértve az elektronikus levelet is) kifejezetten kéri tőle.
(6) A központi adatkezelést végző szervezeti egység adatvédelmi referense számára az (5) bekezdésben előírt nyilvántartás-vezetési kötelezettség az alábbi adatok nyilvántartását írja elő:
a) az adatkezelést végző szervezeti egység megnevezése és
b) az a) pontban megjelölt szervezeti egységnek a konkrét adatkezeléshez kijelölt kapcsolattartója, és
c) a jogos érdeken alapuló adatkezelés megnevezése és
d) a jogos érdeken alapuló adatkezelés során az adatok megőrzési ideje és
e) magát az érdekmérlegelést tartalmazó dokumentumot.
(7) Jogos érdek lehet különösen – az (1) bekezdésben írtak mérlegelése mellett
a) az Egyetemi munkafolyamatok hatékony koordinációja érdekében az Egyetemmel bármilyen foglalkoztatási jogviszonyban álló személy neve, ellátott feladatkörük, munkahelyi postai, illetve e-mail címük, a foglalkoztató szervezeti egység megnevezése, munkahelyi telefonszámuk kezelése.
b) az esetleges csalások, visszaélések megelőzése, vizsgálata céljából kezelt olyan személyes adat, amelyek a csalás, visszaélés megelőzéséhez, vizsgálatához feltétlenül szükséges és még éppen elégséges. A csalások, visszaélések megelőzése és vizsgálata, akkor jogszerű, ha a munkáltatói ellenőrzés szabályait (különösen a munkáltatói ellenőrzés során kezelt személyes adatokat) az Egyetem írásban rögzíti jelen Szabályzat – különösen annak 6. §-ának – figyelembe vételével.
c) szerződésekben kapcsolattartóként megjelölt személyek kapcsolattartási adatai.

### *Jogi kötelezettség teljesítése*

25. §

*[Kapcsolódó jogi háttér: GDPR (45) preambulumbekezdés, 6. cikk (1) bekezdés c) pontja]*

(1) Jogi kötelezettséget, mint jogalapot
a) európai uniós jog vagy
b) magyar jogi norma
állapít meg.
(2) Jogi kötelezettségen alapuló adatkezelések különösen a felsőoktatási tevékenységgel, a foglalkoztatással, a könyvtári és levéltári folyamatokkal, a köznevelési tevékenységgel, valamint az egészségügyi szolgáltatások nyújtásával összefüggő olyan nyilvántartási, valamint jelentési kötelezettségek, amelyek esetében a kötelezően nyilvántartandó, jelentendő adatokat és az adatkezelés körülményeit a jogszabályok taxatív módon meghatározzák.

(3) Jogi kötelezettség-teljesítés jogalapja nem alkalmazható, ha
a) hiányzik a jogi kötelezettség-teljesítés jogalapjának fogalmi kelléke a jogi kötelezettség megléte. A jogi kötelezettség megléte, mint állam által kikényszeríthető magatartási szabály azt jelenti, ha az adatkezelő nem jár el az előírtaknak megfelelően, őt joghátrány éri. Amennyiben erről nincs szó, a jogi kötelezettség-teljesítése jogalapja nem állja meg a helyét.
b) a jogszabály ugyan rögzíti az adatkezelés tényét, de az adatkezelő számára a konkrét adatkezelési tevékenység nem, vagy csupán részlegesen világos. Amennyiben az adatkezelő maga határozza meg az adatkezelés egyes körülményeit, akkor nem a jogi kötelezettség-teljesítés jogalapját, hanem más jogalapot szükséges választani.
c) már – teljes egészében, vagy az adatkezelésre vonatkozóan részlegesen – hatályát veszítette az a jogszabály, amely az Egyetemet adatkezelésre kötelezi.
(4) A kötelező nyilvántartásért felelős szervezeti egység feladata, hogy az adott adatkezelés vonatkozásában naprakészen kövesse a jogszabályi változásokat, és a nyilvántartást a mindenkori jogszabályi előírásoknak megfelelően végezze.
(5) A szervezeti egység vezetője felel azért, hogy az adott szervezeti egységen belül a konkrét adatkezelést végző személyeket naprakészen tájékoztassa, hogy van-e olyan szakmai jogszabályi háttere az adatkezelési tevékenységnek, amely a jogi kötelezettség-teljesítés jogalapjának használatát indokolja, továbbá jelölje meg egyértelműen melyik ez a jogszabály és pontosan milyen kötelezettséget ró az adatkezelést végzőkre.
(6) Amennyiben a szervezeti egység vezetője (5) bekezdésben rögzített kötelezettsége kapcsán bizonytalan
a) az alkalmazandó szakmai jogi háttér tekintetében, megkereséssel élhet a JII felé, vagy egészségügyi adatkezelési tevékenység kapcsán a KK Jogi Osztálya felé.
b) a jogi kötelezettség-teljesítés jogalapjának jogszerű alkalmazása kapcsán, a szakmai jogszabályi háttér megjelölésével, megkereséssel élhet a DPO felé.

### *Szerződéses jogalap*

26. §

*[Kapcsolódó jogi háttér: GDPR (44) preambulumbekezdés, 6. cikk (1) bekezdés b) pontja]*

(1) A szerződés teljesítése, mint adatkezelési jogalap megállapítására akkor kerülhet sor, ha
a) az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik szerződő fél vagy
b) az adatkezelés a szerződés megkötését megelőzően, az érintett kérésére történő lépések megtételéhez szükséges.
(2) Figyelemmel az (1) bekezdésben írtakra, szerződéses adatkezelés lehet különösen valamely adatkezelést végző szervezeti egység szerződéses folyamataihoz kapcsolódó adatkezelés, valamint az adatkezelést végző szervezeti egység által nyújtott, ingyenesen vagy térítés ellenében igénybe vehető szolgáltatás során történő adatkezelés.

### *Létfontosságú érdek jogalapja*

27. §

*[Kapcsolódó jogi háttér: GDPR (46) preambulumbekezdés, 6. cikk (1) bekezdés d) pontja]*

(1) A létfontosságú érdek akkor érvényes jogalap, amikor az érintett vagy egy másik természetes személy élete, test

i épsége veszélybe kerülne az adatkezelés hiányában.
(2) Létfontosságú érdeken alapuló adatkezelést jelent különösen az érintett személy legközelebbi hozzátartozójának a telefonszám-kezelése annak érdekében, hogy az érintett esetleges hirtelen rosszulléte vagy balesete következtében egészségügyi helyzetéről tájékoztatást lehessen adni, vagy ellátása érdekében felvilágosítást lehessen kérni tőle.

### *Közérdek, mint jogalap*

28. §

*[Kapcsolódó jogi háttér: GDPR (46) preambulumbekezdése, 6. cikk (1) bekezdés e) pontja]*

(1) Közérdekűségre történő jogalapi hivatkozás akkor jogszerű, ha az Egyetem közfeladatához kapcsolódik. Az Egyetem alaptevékenységei közérdekű feladatnak minősíthetők (például oktatás, kutatás, betegellátás).
(2) Az adatkezelést végző szervezeti egység felelőssége megítélni, hogy adott adatkezelési tevékenység mennyiben kapcsolódik az Egyetem alaptevékenységéhez.
(3) Az Egyetem alaptevékenységének megítélésében különösen az alapítványi felsőoktatási intézményekre vonatkozó irányadó jogi környezet előírásai, az Egyetem Alapító Okirata, valamint az Egyetem SZMr-je az irányadó.
(4) Közérdek jogalapjának alkalmazhatósága tekintetében felmerülő kérdés kapcsán az adatkezelést végző megkereséssel élhet a DPO felé.

### *Érintettek jogai*

29. §

*[Kapcsolódó jogi háttér: GDPR III. fejezet]*

(1) Az Egyetem adatkezelési tevékenységében érintett személyeket az alábbi jogok illetik meg általánosságban, úgymint
a) a tájékoztatáshoz való jog,
b) a hozzáféréshez való jog,
c) a helyesbítéshez való jog,
d) a tiltakozáshoz való jog,
e) a korlátozáshoz való jog,
f) a törléshez való jog,
g) az adathordozhatóság joga,
h) a jogorvoslathoz való jog.
(2) Az adott adatkezelési tevékenység során konkrétan gyakorolható érintetti jogokat az adott adatkezelési tevékenység jogalapja határozza meg. Ezért az adatkezelést végző szervezeti egységnek különösen körültekintően szükséges eljárnia a jogalapok meghatározása kapcsán. Az érintettek az adott adatkezelési tevékenység során konkrétan gyakorolható érintetti jogaikat az adatkezelési tájékoztatóból ismerhetik meg.

30. §

*[Kapcsolódó jogi háttér: GDPR (64) preambulumbekezdés, valamint 12. cikk]*

(1) Az érintetti jogok gyakorlását – jelen Szabályzat 35. és 36. §-aiban leírt általános és speciális tájékoztatáshoz való jog kivételével – az Egyetem akár szóban (személyesen vagy telefon vagy speciális körülményekre tekintettel – különösen járványügyi helyzetben – az Egyetem által adatbiztonság szempontjából jóváhagyott videóhívás útján), akár írásban (papíralapon vagy elektronikus úton) előadott kérelemre biztosítja kizárólag az érintett azonosítását követően. Az azonosítás jellege függ az érintettről kezelt személyes adatok jellegétől, típusától.
(2) Az érintett papíralapon aláírásával ellátott kérelemben, és az azonosítására szolgáló (5) bekezdés szerinti alapparaméterek megadásával érvényesítheti a jogait.
(3) Elektronikus úton történő joggyakorlás esetén az érintett az Egyetem által (pl. tanulmányi rendszerben, kórház informatikai rendszerben, könyvtár-beiratkozási rendszerben stb.) nyilvántartott, illetve a számára a jogviszonyának kezdetén biztosított, hivatalos elektronikus levelezési címéről küldött üzenetben teheti ezt meg az azonosítására szolgáló (5) bekezdés szerinti alapparaméterek megadásával.
(4) Az érintettek az elektronikus úton történő joggyakorlás esetén a harmadik országban működő levelezőrendszert üzemeltető szolgáltatók igénybe vételének kockázatát maguk viselik. Az Egyetem kifejezetten javasolja, hogy az érintett az Egyetemmel történő elektronikus levelezésre olyan szolgáltatót válasszon, amely a GDPR előírásait maradéktalanul betartja.
(5) Az azonosításra szolgáló alapparaméterek különösen az alábbiak:
a) név, születési név, születési hely és dátum, (ha szükséges az adatkezelést végző szervezeti egység adatkezelése érdekében), édesanyja neve (ez utóbbi opcionális, amennyiben a név nem egyértelműen azonosítja az adott személyt), illetve
b) amennyiben az érintetti joggyakorlás olyan rendszerben tárolt adatokra vonatkozik, amelyben az érintett személy egyedi azonosítóval rendelkezik (Neptun, CooSpace, Nexon, eMedSolution, stb.), akkor a nevének és az azonosítójának megadásával érvényesítheti jogait.
(6) Személyes kommunikáció során az azonosítás elvégezhető az alábbi lehetőségek egyikével:
a) A személyes megjelenéskor az azonosítás elvégezhető az azonosításra szolgáló fényképes igazolvánnyal (pl. diákigazolvány, fényképes egyetemi azonosító kártya, személyazonosító igazolvány). Az azonosítás a megtekintést és – amennyiben erre a belső eljárásrend okán szükség van – az okmány típusának rögzítését jelenti. Az okmányok lemásolása jogszerűtlen, tilos.
b) A személyes ügyintézés során az azonosítás elvégezhető az ügyintéző és az érintett személyes ismeretsége alapján, amennyiben legalább egyszer az azonosítás jelen bekezdés a) pontjában leírt módon már megtörtént.
c) A telefonon történő ügyintézés esetében az azonosítás jelszó használatával történik, amennyiben az érintett az adatkezelést végző szervezeti egység felé előzetesen, írásban, kifejezetten az azonosítására felhasználni kívánt jelszót adott le, és legalább a jelszó-leadásakor jelen bekezdés a) pontjában leírt módon az érintett azonosítása megtörtént. A jelszó az érintett személyes adatát nem tartalmazhatja, az érintett ennek figyelembevételével adhatja meg a jelszót.
d) Videóhívás során az azonosítás elvégezhető olyan módon, hogy az érintett egy személyazonosításra szolgáló fényképes igazolványt mutat fel (pl. diákigazolvány, fényképes egyetemi azonosító kártya, személyazonosító igazolvány), amelyen szereplő

fényképet az ügyintéző összehasonlítja a hívó arcképével. Az azonosítás biztonságosságának növelése érdekében az ügyintéző elkéri az érintett egyik egyetemi belső azonosítóját (pl. Neptun-kód, MedSol azonosító, vagy e-mail cím).
(7) Az érintett azonosítása során az Egyetem az adattakarékosság és a fokozatosság elvének megfelelően jár el, így az azonosítás során az azonosításhoz szükséges adatok köre annak megfelelően kerül meghatározásra, hogy az Egyetemnek megalapozott kétségei merülnek-e fel a kérelmező személyazonosságát illetően.

31. §

*[Kapcsolódó jogi háttér: GDPR 12. cikk (3) bekezdés]*

(1) A központi adatkezelést végző szervezeti egység a hozzá beérkező kérelmet köteles indokolatlan késedelem nélkül, legfeljebb a kérelem benyújtásától számított 28 napon belül az érintetti joggyakorlás tekintetében intézkedni és a kérelmezőt tájékoztatni. A jogszerű intézkedésben tanácsadás kérhető a DPO-tól. Az érintett számára a válaszelőkészítés a JII feladata. A kérelmet kézhez vevő adatkezelést végző szervezeti egység küldi ki az érintett felé a választ.
(2) Az (1) bekezdésben megjelölt határidő szükség esetén – a kérelem tartalmára, annak összetettségére tekintettel – meghosszabbítható a meghosszabbítás okának megjelölésével, legfeljebb 60 nappal. A meghosszabbításról az érintett személyt a kérelmének beérkezésétől számított 28 napon belül kell értesíteni.
(3) Figyelemmel az adatok jellegére és az adatbiztonság követelményeire, az érintetti joggyakorlás tekintetében mindig azon a csatornán keresztül kell az érintett személlyel kommunikálni, amelyet az érintett a kérelmének leadására kiválasztott, kivéve, ha az érintett a választ egy általa meghatározott más csatornán kéri.

32. §

*[Kapcsolódó jogi háttér: GDPR (59) preambulumbekezdés, 12. cikk (5) bekezdés, 15. cikk (3) bekezdés]*

(1) Az érintetti tájékoztatást, joggyakorlást díjmentesen kell megtenni, illetve biztosítani.
(2) Az (1) bekezdésben rögzített díjmentesség alól az alábbi kivételek kerülnek meghatározásra:
a) amennyiben az érintett kérelme egyértelműen megalapozatlan (különösen annak ismétlődő jellegére tekintettel) vagy túlzó, az adatkezelést végző szervezeti egységnek jogában áll észszerű összegű díjat felszámítani, vagy megtagadhatja az érintetti kérelem alapján történő eljárást. Az adatkezelést végző szervezeti egységet terheli a megalapozatlan, illetve túlzó jelleg bizonyítása.
b) az érintett személyt a másolathoz való jog alapján csupán egyszer illeti meg a díjmentesség ugyanazon tárgykörben, a további másolatokért az adatkezelést végző szervezeti egység adminisztratív költségeken alapuló ésszerű díjat számíthat fel.
(3) A (2) bekezdésben megjelölt esetekben az érintett személyt a díjköltség felszámításáról, kérelmének teljesítése előtt, tájékoztatni kell, azzal, hogy a kérelmének teljesítésére akkor kerül sor, ha az érintett ezen körülmény tudatában, az adatkezelést végző szervezeti egység értesítését követő legkésőbb 15 napon belül megerősíti a kérelmét az adatkezelést végző szervezeti egység felé.

(4) Az adminisztratív költségtérítés mértékének meghatározása során az alábbi költségelemek vehetők figyelembe:
a) az igényelt adatokat tartalmazó adathordozó költsége (papírköltség, pendrive költsége, stb.), ide értve az adathordozóra mentés, nyomtatás költségét is, valamint
b) az igényelt adatokat tartalmazó adathordozó az igénylő részére történő kézbesítésének költsége.
(5) A (2) bekezdés b) pontjában leírtak megvalósítása érdekében az adatkezelést végző szervezeti egység nyilvántartást vezet az érintetti másolati joggyakorlásról, kivéve a kamerafelvételek, valamint a rögzített telefonhívások kikérését.
(6) A kamerafelvétel másolatának kikéréséről, valamint a rögzített telefonhívásokra vonatkozó érintetti hozzáférés joggyakorlásáról a JII vezet nyilvántartást a Védelmi Irodával együttműködve.

33. §

[*Kapcsolódó jogi háttér: GDPR 12. cikk (4) bekezdés, és 77. cikk, valamint 79. cikk*]

(1) Ha az érintett kérelme nem teljesíthető, az adatkezelést végző szervezeti egység a kérelem kézhezvételét követő legkésőbb 28 napon belül tájékoztatja az érintett személyt és közli a kérelem elutasításának ténybeli és jogi indokait. A válaszelőkészítés a JII feladata.
(2) A kérelem elutasítása esetén az érintettet tájékoztatni kell, az (1) bekezdésben leírtakon túl, a jelen Szabályzat szerinti jogorvoslati lehetőségekről is.

### *Tájékoztatáshoz való jog*

[*Kapcsolódó jogi háttér: GDPR 12-14. cikkei*]

34. §

(1) Az érintetteknek joguk van a tájékoztatáshoz a személyes adataikhoz kötődő adatkezeléssel összefüggő tényekről az adatkezelés megkezdését megelőzően, de legkésőbb a személyes adatok megszerzésének időpontjában.
(2) Kivételes esetben, ha a személyes adat nem az érintett személytől, hanem más forrásból származik, akkor a tájékoztatásra az eset valamennyi körülményére figyelemmel a lehető leghamarabb, de legkésőbb az alábbiak szerint kerül sor:
a) a személyes adatok kezelésének konkrét körülményeit tekintetbe véve, a személyes adatok megszerzésétől számított észszerű határidőn, de legkésőbb egy hónapon belül,
b) ha a személyes adatokat az érintett személlyel való kapcsolattartás céljára használják, legalább az érintett személlyel való első kapcsolatfelvétel alkalmával, vagy
c) ha várhatóan más címzettel is közlik az adatokat, legkésőbb a személyes adatok első alkalommal való közlésekor.
(3) A tájékoztatáshoz való jogukat az érintettek az alábbi módokon gyakorolhatják:
a) a Szabályzat 35. §-ában rögzített általános tájékoztatáshoz való jog formájában, és
b) a Szabályzat 36. §-ában leírt speciális tájékoztatáshoz való jog formájában, valamint
c) a Szabályzat 37. §-ában ismertetett egyedi tájékoztatáshoz való jog formájában (ún. hozzáférés jogának gyakorlásával).

(4) Az általános, valamint a specializált tájékoztatást minden esetben az adatkezelés megkezdése előtt, de legkésőbb az (1) és (2) bekezdésben foglaltak szerint kell megtenni, így különösen az alábbi esetekben és módon:
a) az Egyetemre álláspályázatot benyújtók számára az álláspályázati felhívásban,
b) az Egyetemmel munkavégzésre irányuló jogviszonyt létesítő személyek részére a jogviszony létrejöttekor,
c) az Egyetem által működtetett óvoda, gyakorló általános iskola és gimnázium tanulójának törvényes képviselőjét a felvételi jelentkezéskor, legkésőbb a beiratkozás során,
d) az Egyetemre felvételi jelentkezést benyújtók részére a felvételi tájékoztató keretében,
e) az Egyetemmel tanulói, hallgatói, doktorjelölti jogviszonyt létesítő személyek részére az Egyetemre beiratkozásuk alkalmával,
f) a habilitációs eljárás lefolytatása iránti kérelem leadása előtt az eljárásról szóló tájékoztatás során,
g) a doktori fokozatszerzési eljárásra történő jelentkezési lap leadása előtt az eljárásról szóló tájékoztatás során,
h) az Egyetem infrastruktúráját használó személyek számára a személyes adat kezelésének megkezdését megelőzően,
i) az Egyetem által szervezett felnőttképzésre való jelentkezés esetén a jelentkezési felhívásban,
j) a rendezvények, események, workshop-ok kapcsán a személyes adatkezelés első állomását megelőzően (pl. regisztrációköteles rendezvények esetében a regisztrációs felületen az adatok megadásának megkezdését megelőzően),
k) belső oktatás esetén legkésőbb az oktatáson készített jelenléti ív felvételekor,
l) a betegellátásra jelentkező érintetteket első jelentkezésük alkalmával,
m) tudományos kutatás potenciális alanyai a kutatásvezető által készített, elektronikusan is közzétett tájékoztatást kell kapjanak a kutatás megkezdése előtt.
(5) A tájékoztatást magyar anyanyelvű személyek esetén magyar nyelven, a nem magyar anyanyelvű személy esetében az Egyetemmel létrejövő jogviszonynak megfelelő munkanyelven (pl. az adott képzés nyelvén, a szolgáltatásnyújtás általános munkanyelvén) kell megtenni. Amennyiben az Egyetem a munkanyelven keresztül biztosította a tájékoztatást, nem köteles az érintett anyanyelvére is lefordítani azt.

### *Általános tájékoztatás*

35. §

(1) Az általános tájékoztatás keretében az érintettek az adatvédelmi előírásokról az alábbi forrásokból tájékozódhatnak:
a) jelen Szabályzatból, valamint
b) az elfogadásra kerülő eljárásrendekből.
(2) A tanulói, a hallgatói beiratkozási lap, továbbá a foglalkoztatási jogviszonyhoz, valamint az adatkezeléshez kapcsolható egyéb szerződések kötelező tartalmi eleme annak elismerése az Egyetemmel jogviszonyt létesítő fél részéről, hogy az Egyetem vonatkozó szabályzatainak rendelkezését megismerte és magára nézve kötelezően elfogadja.

### *Speciális tájékoztatás*

36. §

*[Kapcsolódó jogi háttér: GDPR (58), (60)-(61), (63) preambulumbekezdés]*

(1) Speciális tájékoztatás formájában gyakorolja az érintett a tájékoztatáshoz való jogát a személyes adatainak kezelése esetén elkészített adatkezelési tájékoztató elolvasásával és megismerésével.
(2) Amennyiben az adott eseményhez, folyamathoz személyes adatkezelés kapcsolódik, akkor adatkezelési tájékoztató elkészítése nélkül az adott esemény lebonyolítása adatvédelmi szempontból nem jogszerű. Ilyen esetben az érintettnek jogában áll a DPO felé panaszt tenni, függetlenül attól, hogy ugyanebben az ügyben esetlegesen az Adatvédelmi Hatóság vagy bíróság eljárását is kezdeményezte.
(3) Az adatkezelési tájékoztató elkészítése az adatkezelést végző szervezeti egység feladata. Az adatkezelést végző szervezeti egység felel az adatkezelési tájékoztató formai és tartalmi megfelelőségéért.
(4) Az adatkezelési tájékoztató kötelező eleme az adatkezelést végző szervezeti egység, az adatkezelési tájékoztatóban ismertetett adatkezelési folyamat szakmai kapcsolattartójának, valamint az adatkezelést végző szervezeti egység adatvédelmi referensének megnevezése. Szakmai kapcsolattartónak olyan személyt szükséges kijelölni, akitől az érintett az adott adatkezelés gyakorlati kivitelezése kapcsán tehet fel kérdést. Az érintett az egység adatvédelmi referensén keresztül is érvényesítheti jogait az Egyetemmel szemben, különös tekintettel a hozzáféréshez való jogot, mint egyedi tájékoztatáshoz való jogát, vagy az adott adatkezelés során esetlegesen fennálló tiltakozáshoz való jogát. A szakmai kapcsolattartó és az egység adatvédelmi referense köteles együttműködni, és elősegíteni az érintetti joggyakorlást, illetve informálódását, még akkor is, ha az érintett felcseréli a két szerepkört megkeresésében.
(5) A JII feladata a GDPR előírásainak megfelelő, az adatkezelési tájékoztató elkészítéséhez szükséges mintadokumentum létrehozatala magyar és angol nyelven, valamint azok naprakészen tartása.
(6) A JII az adatkezelést végző szervezeti egység adatvédelmi referense részére a mindenkori jogi környezetnek megfelelő adatkezelési tájékoztató mintadokumentumot eljuttatja. Az adatkezelési tájékoztató mintát az adott adatkezelést végző szervezeti egységbe tartozók az adatkezelést végző szervezeti egység adatvédelmi referensétől kérhetik el.
(7) Az adatkezelést végző szervezeti egység a JII által elkészített és az adatkezelési tájékoztató összeállításakor hatályos adatkezelési tájékoztató mintát köteles használni.
(8) Más folyamat, esemény, rendezvény adatkezelési tájékoztatójának változatlan formában történő átvétele nem megengedett, tekintettel arra, hogy az adatkezelések hasonló jellegű folyamatok, események, rendezvények esetében is eltérhetnek egymástól (megváltoztatva ezzel különösen a kezelt adatok körét, célját, jogalapját, megőrzési idejét, valamint az érintett jogait), továbbá az elkészített adatkezelési tájékoztatók az elkészítésük időpillanatában hatályos jogi környezeten és mintadokumentáción alapulnak.

### *Hozzáférés joga*

37. §

*[Kapcsolódó jogi háttér: GDPR (63) preambulumbekezdése, 15. cikk]*

(1) Az érintett jogosult arra, hogy kérelmére személyes adatait és az azok kezelésével összefüggő információkat az adatkezelést végző szervezeti egység a rendelkezésére bocsássa.
(2) A hozzáféréshez való joga keretében az érintett jogosult saját személyes adatairól másolatot kapni.
(3) A hozzáféréshez való jogot (ideértve a másolathoz való jogot is) minden esetben úgy kell biztosítani, hogy ezalatt az érintett más személy személyes adatait ne ismerhesse meg.
(4) Az érintett a hozzáférés jogának (másolathoz való jog) gyakorlása keretében különösen az alábbiakra jogosult:
a) az Egyetem bármely elektronikus nyilvántartó rendszeréből kikérheti a rá vonatkozó személyes adatok másolatát,
b) az Egyetem bármely elektronikus nyilvántartó rendszeréből a saját személyes adatai vonatkozásában kikérheti a felhasználói tevékenységet tartalmazó naplófile kivonatot,
c) az Egyetem által rögzített telefonhívás esetén, az érintett, a megőrzési időn belül, kikérheti saját hívásának hangfelvételét,
d) az Egyetem területén működő kamerák tekintetében saját magára vonatkozóan kikérheti a kamerafelvétel másolatát,
e) elektronikus beléptetőrendszer használata esetén kikérheti saját magára vonatkozóan a be- és kilépéseinek nyilvántartás-másolatát,
f) a tanulói, hallgatói jogviszonyban állók írásbeli dolgozataikba, vizsgáikba, szakdolgozati bírálataikba beletekinthet és másolatot kérhet róluk,
g) a KK betegei a róluk vezetett egészségügyi dokumentációba betekinthetnek, illetve másolatot kérhetnek a dokumentumokról. Ezt a jogot az Eütv., valamint az Eüak. előírásainak figyelembevételével gyakorolhatják.
(5) Az érintett hozzáférési jogának gyakorlása tárgyában benyújtott kérelmének teljesítésére az adatkezelést végző szervezeti egység köteles.
(6) A kamerafelvétel, valamint a rögzített telefonhívások másolatának kikérése minden esetben a Védelmi Irodán keresztül történik a JII bevonásával.

### *Helyesbítéshez való jog*

38. §

*[Kapcsolódó jogi háttér: GDPR 16. cikk]*

(1) Adatváltozás vagy téves adatrögzítés észlelése esetén az érintett kérheti kezelt adatainak kiegészítését, illetve kijavítását.
(2) Az adatkezelést végző szervezeti egység feladata annak megszervezése, hogy az érintett helyesbítési kérelmében megjelölt adatkör vonatkozásában az adatkezelést végző szervezeti egység általa használt adatbázisok, nyilvántartások lehető legszélesebb körére nézve megoldja a helyesbítést, amennyiben a kérelemben megjelölt adatkör más adatbázis, nyilvántartás része is.

(3) Az Egyetem az adatkezelést végző szervezeti egység útján minden olyan címzettet tájékoztat a helyesbítésről, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére az adatkezelést végző szervezeti egység tájékoztatja a címzettekről.
(4) Meg nem történt eseményre vonatkozó, vagy nyilvánvalóan valótlan adat esetén a helyesbítésen az adat törlését kell érteni.
(5) A kép-és hangfelvételek vonatkozásában fogalmilag kizárt a helyesbítés jogának érvényesítése.

### *Tiltakozáshoz való jog*

39. §

*[Kapcsolódó jogi háttér: GDPR 21. cikk]*

(1) Az érintett jogosult a közérdeken vagy jogos érdeken alapuló adatkezelés esetén a saját helyzetével kapcsolatos okokból tiltakozni személyes adatainak kezelése ellen, ideértve az adatkezelés tényleges megkezdését megelőzően megtett tiltakozást és a profilalkotást is.
(2) Az (1) bekezdésben leírt tiltakozáshoz való jog érvényesítése esetén, az Egyetem az érintettre vonatkozó személyes adatokat nem kezelheti, vagy nem kezelheti tovább, kivéve, ha az Egyetem bizonyítja, hogy a tiltakozásban megjelölt
a) adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy
b) adatkezelés jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy mások által előterjesztett jogi igény elleni védekezéshez kapcsolódik. Az ilyen adatkezelések során is be kell tartani a szükségesség, arányosság, valamint a célhoz kötöttség követelményét.

### *Korlátozáshoz való jog*

*[Kapcsolódó jogi háttér: GDPR 18. cikk]*

40. §

(1) Az érintett jogosult arra, hogy az Egyetem által kezelt személyes adatai vonatkozásában korlátozza az adatkezelést, amennyiben
a) vitatja az adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az adatkezelő ellenőrizze a személyes adatok pontosságát, vagy
b) vitatja az adatkezelés jogszerűségét, de ellenzi azok törlését, és ehelyett kéri azok felhasználásának korlátozását, vagy
c) jogi igényének érvényesítéséhez és védelméhez igényli azt, azonban az adatkezelőnek már nincs az adatokra szüksége, vagy
d) tiltakozott az adatkezelés ellen, de még nem került megállapításra, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.
(2) A korlátozáshoz való jog addig tart, amíg az adatkezelést végző szervezeti egység megvizsgálja az érintett által a korlátozáshoz való jog érvényesítésének indokaként az érintetti kérelemben megjelölt okot.

(3) Az adatkezelést végző szervezeti egység az érintetti kérelem megalapozottsága esetén azonnal intézkedik az érintetti kérelem végrehajtásáról.
(4) Amennyiben az érintetti kérelem megalapozatlan, úgy az adatkezelést végző szervezeti egység intézkedik a korlátozás feloldásáról, és erről az érintett személyt előzetesen, legalább 15 nappal az adatkezelés megkezdését megelőzően, tájékoztatja.

### *Törléshez való jog*

*[Kapcsolódó jogi háttér: GDPR (156) preambulumbekezdése, és a 17. cikk, valamint a 89. cikk]*

41. §

(1) Az érintett jogosult arra, hogy az adatkezelő által kezelt személyes adatainak törlését kérje, ha
a) a személyes adat kezelésére már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték, vagy
b) az adatkezelés az érintett hozzájárulásán alapult, és az adatkezelésnek nincs más jogalapja, vagy
c) az érintett tiltakozott az adatkezelés ellen és nincs elsőbbséget élvező jogszerű ok az adatkezelésre, vagy
d) személyes adatát az adatkezelő jogellenesen kezelte, illetve kezeli, vagy
e) a személyes adatokat az adatkezelőre alkalmazandó uniós vagy magyar jogban előírt jogi kötelezettség teljesítéséhez törölni kell,
f) a személyes adatok gyűjtésére az információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor.
(2) Nincs helye törlési kérelemnek, ha a kérelemben megjelölt adatkezelés
a) jogszabályon alapul, vagy
b) véleménynyilvánítás szabadságához, illetve a tájékozódáshoz való jog gyakorlása érdekében szükséges, vagy
c) közérdekű feladat ellátásához kapcsolódik, vagy
d) jogi igény érvényesítéséhez, védelméhez kapcsolható, vagy
e) közérdekű archiválás, tudományos kutatás, történelmi kutatás vagy statisztikai célból folytatott adatkezelési folyamatra vonatkozik, amennyiben az adatok törlése valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné az adatkezelést, és amely során igazolható módon garanciákat biztosít az adatkezelést végző szervezeti egység az adatok adatbiztonságára nézve, az adattakarékosság elvének megtartására és arra, hogy az érintett csupán a legszükségesebb mértékben és ideig legyen beazonosítható (pl. álnevesítés vagy anonimizálás módszerének segítségével), vagy
f) az adatkezelés szükséges a GDPR 9. cikk (2) bekezdése h) és i) pontjának, valamint a 9. cikk (3) bekezdésének megfelelően a népegészségügy területét érintő közérdek alapján.

### *Adathordozhatósághoz való jog*

*[Kapcsolódó jogi háttér: GDPR 20. cikk]*

42. §

(1) Az érintett jogosult az Egyetem rendelkezésére bocsátott, rá vonatkozó személyes adatokat széles körben használt elektronikus formában megkapni és az adatokat más

adatkezelő részére továbbítani, amennyiben az adatkezelés automatizált módon történik és az adatkezelés jogalapja
a) az érintett hozzájárulása, vagy
b) olyan szerződés, amelyben az érintett az egyik fél.
(2) Az adatok hordozhatóságához való jog gyakorlása során az érintett jogosult arra, hogy – ha ez technikailag megvalósítható – kérje a személyes adatok adatkezelők közötti közvetlen továbbítását.

### *Jogorvoslathoz való jog*

*[Kapcsolódó jogi háttér: Alaptörvény XXVIII. cikk (7) bekezdés]*

43. §

(1) Az érintett jogosult arra, hogy az általa sérelmesnek tartott adatkezelések tekintetében jogorvoslattal éljen.
(2) A jogorvoslathoz való jogosultság belső, valamint külső jogorvoslati eszközökből áll.
(3) Belső jogorvoslati eszköz az adatvédelmi panasz, valamint az adatvédelmi közérdekű bejelentés. Külső jogorvoslati eszköz az Adatvédelmi Hatósághoz fordulás vagy a bírósági igényérvényesítés.
(4) Az érintett számára adott tájékoztatásokban javasolni kell, hogy az érintett a jogsérelmének orvoslását először a belső jogorvoslati eszközökön keresztül kísérelje meg.

### *Adatvédelmi panasz*

### *Panaszbenyújtás*

44. §

(1) Az érintett jogosult arra, hogy az általa sérelmesnek tartott adatkezelések tekintetében adatvédelmi panasszal éljen az adott adatkezelést végző szervezeti egység vezetője felé. A szóban előterjesztett panaszról az adatkezelést végző szervezeti egység feljegyzést köteles készíteni.
(2) Az adatkezelést végző szervezeti egység vezetője a panaszost a kérelem kézhezvételét követő 28 napon belül írásban tájékoztatja
a) a panasz kivizsgálásának eredményéről, valamint a már megtett, illetve a tervezett intézkedésekről, vagy
b) a panasz elutasításáról megjelölve a panasz elutasításának ténybeli és jogi indokait, valamint jelen Szabályzatban meghatározott jogorvoslati lehetőségekről is.
(3) Ha a panaszolt adatkezelés olyan kérdésre irányul, amely az adatkezelést végző szervezeti egység hatáskörén kívül esik, illetve, ha az adatkezelést végző szervezeti egység előzetes vizsgálata alapján a panasz elutasításának lehet helye, akkor a panaszt az adatkezelést végző szervezeti egység vezetője két munkanapon belül továbbítja állásfoglaláskérés érdekében a DPO-hoz. Amennyiben a panasz megvizsgálásába a DPO bevonásra kerül, akkor a panasz DPO részére történő továbbításakor ezt a tényt a panaszos felé jelezni szükséges, mivel ezzel a Szabályzat 45. §-ában rögzített belső jogorvoslat lehetősége kimerítésre kerül.
(4) A panasz megválaszolását a JII készíti elő az adatkezelést végző szervezeti egység vezetője részére.

### *Adatvédelmi tisztviselőhöz fordulás*

45. §

(1) Az érintett a 44. § alkalmazása helyett jogosult arra is, hogy az általa sérelmesnek tartott adatkezelések tekintetében adatvédelmi panasszal forduljon a DPO-hoz.
(2) A DPO a panaszt megvizsgálja. A vizsgálat keretében a DPO jogköre teljeskörű, joga van különösen, hogy
a) kikérje az adatkezelést végző szervezeti egységtől az ügyben nála keletkezett iratokat, és egyéb, az ügy kivizsgálásához tartozó dokumentációt,
b) az adatkezelést végző szervezeti egység bármely munkatársa számára kérdést tehet fel, illetve tájékoztatást kérhet az általa megjelölt határidőn belül,
c) betekinthet az adatkezelést végző szervezeti egység ügymenetében, nyilvántartásaiba, folyamataiba,
d) az adatkezelést végző szervezeti egység működését, illetve a betegellátás speciális körülményeit figyelembe véve, és az érintettek, különösen a betegek emberi méltóságát tiszteletben tartva, beléphet az adatkezelést végző szervezeti egység bármely helyiségébe.
(3) A vizsgálat alá vont adatkezelést végző szervezeti egység együttműködési kötelezettséggel tartozik a DPO felé.
(4) Az egészségügyi adatvédelmi tisztviselő a hozzá beérkező adatvédelmi panaszt, a kivizsgálás folyamatát és eredményét a DPO-val előzetesen egyezteti.
(5) Amennyiben az adatvédelmi panasz egészségügyi személyes adatra vonatkozik a DPO kikéri az egészségügyi adatvédelmi tisztviselő véleményét.
(6) A DPO a vizsgálat eredményeiről és az általa szükségesnek tartott lépések megtételére vonatkozó javaslatának megfogalmazásával egyidejűleg, tájékoztatja az adatkezelést végző szervezeti egység vezetőjét. Amennyiben a panasszal érintett szervezeti egység helyi adatkezelést végző szervezeti egységnek minősül, a tájékoztatást annak a központi adatkezelést végző szervezeti egység vezetője felé is megteszi, akihez a helyi szervezeti egység tartozik.
(7) A központi adatkezelést végző szervezeti egység a DPO-t tájékoztatja az elrendelt intézkedésekről és a hozzárendelt határidőkről. A DPO tájékoztatja a panaszost az elrendelt intézkedésekről és a hozzárendelt határidőkről a panasz beérkezésétől számított 30 napon belül. Ez a határidő további 30 nappal meghosszabbítható a panasz összetettségére tekintettel. A határidő meghosszabbításáról a panasz beérkezését követő legkésőbb 30 napon belül tájékoztatja a DPO a panaszost.
(8) Amennyiben az adatkezelést végző szervezeti egységnél az intézkedés végrehajtása elháríthatatlan akadályba ütközik, akkor az elháríthatatlan akadály és a megvalósításhoz szükséges új határidő pontos megjelölésével tájékoztatja az intézkedést elrendelőt. Az új határidőnek arányosnak kell lennie a hátráltató akadállyal. Ha az intézkedést elrendelő elfogadja a bejelentést, értesíti erről a DPO-t. A panaszost a DPO tájékoztatja az elháríthatatlan akadály felmerüléséről és az új határidő kijelöléséről.
(9) A szükséges intézkedésre kijelölt szervezeti egység a megvalósulásról írásban tájékoztatja az intézkedés elrendelőjét, valamint a DPO-t.
(10) Amennyiben a DPO nem ért egyet a megvalósításra vonatkozó tájékoztatással, köteles az intézkedés elrendelőjét tájékoztatni erről a beérkezéstől számított 15 napon belül.
(11) A panasz elintézésének időtartama a (8)-(10) bekezdések szerinti esetben sem haladhatja meg a panasz beérkezésétől számított három hónapot.
(12) A DPO tájékoztatja a panaszost az elvégzett intézkedésekről.

(13) Amennyiben a DPO a panasz elutasítására tesz javaslatot és a központi adatkezelést végző szervezeti egység vezetője ezzel egyetért, akkor a panaszost a DPO úgy tájékoztatja, hogy felhívja a figyelmét a bírósági jogorvoslat, továbbá az Adatvédelmi Hatósághoz fordulás lehetőségére.
(14) A DPO-hoz beérkező adatvédelmi panaszok nyilvántartására a 46. §-ban leírtakat szükséges alkalmazni.

### *Adatvédelmi panasz-nyilvántartás*

46. §

(1) Az Egyetem bármelyik szervezeti egységéhez beérkező adatvédelmi panaszt az ahhoz tartozó utolsó vizsgálati cselekmény vagy intézkedés befejezésétől számított 5 évig szükséges megőrizni, ezt követően törölni kell.
(2) Az Egyetem adatvédelmi panasz-nyilvántartását a JII vezeti az (1) bekezdés szerint megjelölt ideig.
(3) Az adatkezelést végző szervezeti egység köteles a hozzá beérkező adatvédelmi panaszról a (4) bekezdésben leírt elemek megjelölésével tájékoztatni az JII-t.
(4) Az adatvédelmi panasz nyilvántartás része különösen:
a) a panasz tárgya,
b) a panasz benyújtásának helye és időpontja,
c) panasz kivizsgálásának körülményei,
d) a panaszos tájékoztatása (a panasz elutasításáról, az elutasítás okairól vagy a szükséges intézkedések megtételéről) és annak időpontja,
e) a panaszhoz tartozó eljárási események,
f) az ügyben megtett utolsó vizsgálati cselekmény, illetve intézkedés dátuma.
(5) A JII-nek joga van felhívni az adatkezelést végző szervezeti egység vezetőjének figyelmét, ha a szervezeti egységhez tartozó adatvédelmi panaszok általános adatvédelmi integritássértésre irányulnak. A szervezeti egység vezetője köteles a számára jelzett adatvédelmi integritássértés orvoslására.

### *Adatvédelmi közérdekű bejelentés*

47. §

(1) Bárki jogosult arra, hogy az általa sérelmesnek tartott adatkezelések tekintetében adatvédelmi közérdekű bejelentéssel éljen a DPO felé.
(2) A közérdekű bejelentő személyes adatai nem tehetők megismerhetővé, annak kezelésére kizárólag a DPO és a JII jogosult, valamint a (3) bekezdésben leírtak megvalósulása esetén az egészségügyi adatvédelmi tisztviselő.
(3) Amennyiben a közérdekű bejelentés egészségügyi személyes adatra vonatkozik, a DPO kikéri az egészségügyi adatvédelmi tisztviselő véleményét a bejelentés tekintetében.
(4) A JII az adatvédelmi közérdekű bejelentés-nyilvántartásban az adatvédelmi közérdekű bejelentést az ahhoz tartozó utolsó vizsgálati cselekmény vagy intézkedés befejezésétől számított 5 évig őrzi, ezt követően pedig törli.
(5) Az adatvédelmi közérdekű bejelentés-nyilvántartás tartalmazza különösen:
a) a bejelentés tárgyát,
b) a bejelentés adatvédelmi tisztviselőhöz beérkezésének időpontját,

c) a bejelentés elutasítását, annak okait és időpontját vagy a szükséges intézkedések megtételét és annak időpontját,
d) bejelentő tájékoztatásának időpontját,
e) az ügyben megtett utolsó vizsgálati cselekmény, illetve intézkedés dátumát.
(6) Az adatvédelmi közérdekű bejelentés tekintetében a DPO mérlegeli, hogy a bejelentéssel érintett ügy, valamint a felmerült jogsértés súlya alapján szükséges-e vizsgálatot indítania. Amennyiben a DPO a vizsgálat megindítását indokoltnak tartja, az adatvédelmi panaszra vonatkozó szabályokat kell alkalmazni a közérdekű bejelentésre nézve, azzal az eltéréssel, hogy a közérdekű bejelentő tájékoztatását minden esetben a DPO végzi el.

### *Adatvédelmi Hatósághoz, valamint bírósághoz fordulás joga*

*[Kapcsolódó jogi háttér: Alaptörvény VI. cikk (4) bekezdés, valamint a GDPR 77-79. §, valamint 82. cikk, továbbá Infotv. 51/A. § (2) bekezdés, 52. §, 60. §, Ptk. 2:43. §, valamint a 2:52-2:53. §-ok]*

48. §

(1) Az érintett személy az Adatvédelmi Hatóságnál hatósági eljárást vagy bíróságnál peres eljárást kezdeményezhet, akkor, ha
a) panaszára sem az adatkezelést végző szervezeti egység, sem a DPO nem reagált az ügyintézésre nyitva álló időn belül, vagy
b) a belső jogorvoslat igénybevétele során a DPO tájékoztatásával, intézkedésével nem ért egyet, vagy
c) az intézkedés végrehajtására az adatkezelést végző szervezeti egység számára kijelölt határidő, kimentés közlése nélkül, eredménytelenül telik el.
(2) Az (1) bekezdésben leírtakon túl Adatvédelmi Hatóságnál bárki vizsgálati eljárást kezdeményezhet arra való hivatkozással, hogy a személyes adatok kezelésével kapcsolatban jogsérelem következett be, vagy annak közvetlen veszélye fennáll.
(3) Bíróságon peres eljárást az (1) bekezdésben leírtakon kívül az is kezdeményezhet, akinek igazolható érdeke fűződik a jogsérelem megállapításához.
(4) Minden olyan személy, aki az adatvédelmi szabályok megsértése révén személyes adatainak védelméhez való jog tekintetében
a) sérelmet szenved, sérelemdíjat,
b) jogellenesen kárt szenved, kártérítést
követelhet a bíróság előtt az adatkezelőtől.

## II. ADATKEZELÉS

*[Kapcsolódó jogi háttér: GDPR (74) preambulumbekezdés, valamint 5. cikk (2) bekezdése, továbbá 12. cikk (1) bekezdés]*

### *Az Egyetem, mint adatkezelő*

49. §

(1) A Szabályzat hatálya alá tartozó adatkezelési tevékenységek vonatkozásában minden esetben az Egyetem minősül adatkezelőnek.
(2) Az Egyetem az (1) bekezdés szerinti adatkezeléseket az erre felhatalmazott adatkezelést végző szervezeti egységek munkatársai útján valósítja meg.

### *Adatfeldolgozó igénybevétele*

*[Kapcsolódó jogi háttér: GDPR (79), (81), és a (83), illetve a (95) preambulumbekezdés, valamint 28-29. cikkek, továbbá a 30. cikk (2) bekezdése]*

50. §

(1) Az Egyetem az egyes adatkezelési műveletek végrehajtására igénybe vehet adatfeldolgozót. Az adatfeldolgozó az Egyetem, mint adatkezelő nevében, annak megbízásából és utasításai szerint végzi tevékenységét, írásban megfogalmazott adatfeldolgozási szerződés alapján.
(2) A központi adatkezelést végző szervezeti egység feladata, hogy adatkezelési tevékenységek tekintetében adatfeldolgozási szerződést készítsen, és azt naprakészen tartsa.
(3) A központi adatkezelést végző szervezeti egység köteles meggyőződni arról, hogy az általa igénybe vett adatfeldolgozó megfelelő adatvédelmi és adatbiztonsági garanciákat nyújtva végzi az adatkezelési tevékenységet. Ennek megítéléséhez a központi adatkezelést végző szervezeti egység adatvédelmi megfelelés megállapítása érdekében megkereséssel élhet a DPO felé, valamint az adatbiztonsági megfelelés megállapítása érdekében az információbiztonsági felelős felé, akik a megkereséstől számított 30 napon belül állásfoglalást bocsátanak ki az adatvédelmi, illetve az adatbiztonsági megfelelés kapcsán. Az eljárási idő az ügy körülményeire tekintettel további 30 nappal meghosszabbítható.
(4) Az adatfeldolgozást végző megnevezése az adott adatkezelési folyamatra készített adatkezelési tájékoztató kötelező eleme.
(5) Az adatfeldolgozási szerződésnek tartalmaznia kell a GDPR 28. § cikkének (3) bekezdése szerinti előírásokat, így különösen:
a) az adatkezelő és az adatfeldolgozó szerepkörök tisztázása, és a beazonosításukhoz szükséges adatok,
b) az adatfeldolgozás célja,
c) az adatfeldolgozás tárgya,
d) az adatfeldolgozáshoz tartozó személyes adatok típusa (ún. adatkörök)
e) az adatfeldolgozás időtartama,
f) az érintettek kategóriái,
g) az adatok átadásának módja és jellege (különösen, hogy hol keletkeznek az adatok, rendszeres, időszakos vagy egyszeri adatátadásról van-e szó, milyen módon kerül az adatfeldolgozóhoz az adat)

h) az adatfeldolgozási feladat pontos és részletes leírása (mit tehet, és mit nem tehet az adatfeldolgozó a személyes adatokkal),
i) adatkezelő és adatfeldolgozó jogai és kötelezettségei, különösen:
- adatbiztonsági garanciák,
- további adatfeldolgozó igénybevételének szabályai,
- adatfeldolgozó adatkezelői ellenőrzése,
- nyilvántartásvezetési kötelezettségek,
- adatkezelési tájékoztató elkészítése,
- az adatvédelmi együttműködés rögzítése (mi az eljárás egy esetleges adatvédelmi incidens esetén vagy az érintett jogainak gyakorlása kapcsán),
- felelősségi kérdések (titoktartás, jogsértés következményei)
- utasításadás körülményei és azok betartásának szabályai, jogsértő utasítással szembeni fellépés,

j) eljárás a szerződés megszűnésekor (különös tekintettel az adatfeldolgozással érintett személyes adatok sorsára vonatkozóan, amelyeket az adatfeldolgozó törölni köteles, vagy visszaszármaztatni az adatkezelőnek).
(6) Az adatfeldolgozással nem bízható meg olyan szervezet, amely a feldolgozandó személyes adatokat felhasználó üzleti tevékenységben érdekelt.
(7) Az adatfeldolgozásra irányuló szerződésekre egyebekben az Egyetem belső szabályzói szerinti szerződéskötési szabályok irányadóak.
(8) Adatfeldolgozás történhet jogszabályi előírás alapján is, ez esetben az adatfeldolgozási jogviszonyra a jogszabályi előírások az irányadók. Nem szükséges írásbeli megállapodást kötni, amennyiben az adatfeldolgozási jogviszonyt az adott jogszabály teljeskörűen szabályozza.
(9) A JII feladata, hogy adatfeldolgozási mintaszerződést készítsen és azt az adatvédelmi referensek számára elérhetővé tegye.

### *Az Egyetem, mint adatfeldolgozó*

*[Kapcsolódó jogi háttér: GDPR (79), (81) és a (83), illetve a (95) preambulumbekezdés, valamint 28-29. cikkek, továbbá a 30. cikk (2) bekezdése]*

51. §

Az Egyetem az adatfeldolgozási tevékenységét erre felhatalmazott szervezeti egységek munkatársai útján valósítja meg.

52. §

(1) Az adatkezelő adatvédelmi elvárásait a DPO-val, az adatkezelő adatbiztonsági elvárásait az információbiztonsági felelőssel előzetesen, mielőbb, de legalább az adatfeldolgozási szerződés megkötését, illetve módosítását megelőző 30 nappal az adatfeldolgozással érintett központi adatkezelést végző szervezeti egység egyezteti.
(2) Az Egyetem, mint adatfeldolgozóval megkötendő adatfeldolgozási szerződésre is irányadó jelen Szabályzat 50. § (5) bekezdésében felsorolt, kötelező szerződés-elemek, azzal a megkötéssel, hogy az Egyetem adatfeldolgozói szerepkörében – tekintettel jelen szakasz

(3) bekezdésében előírtak teljesítésére – az adatkezelő által szabott keretek között köteles eljárni, és köteles alkalmazkodni az adatkezelő elvárásaihoz, beleértve ebbe az adatfeldolgozási szerződés tartalmát is.
(3) Az adatfeldolgozással érintettszervezeti egység, mint adatkezelést végző szervezeti egység köteles haladéktalanul tájékoztatni az adatkezelőt, ha úgy véli, hogy valamely utasítása, eljárása az adatvédelmi jogszabályokat sérti.
(4) Amennyiben az adatfeldolgozó az adatvédelmi szabályokat megsértve maga határozza meg az adatkezelés célját és eszközeit, akkor az adott adatkezelés vonatkozásában őt adatkezelőnek kell tekinteni, és a felelősségét ez alapján szükséges megítélni.
(5) Amennyiben az adatkezelő kérés ellenére sem ad módszertani útmutatást az Egyetem számára az adatfeldolgozással érintett személyes adatokra vonatkozó adatkezelési tevékenységek nyilvántartására, akkor a DPO ad módszertani útmutatót ehhez.

### *Szerződéskötés általános adatvédelmi elvárásai*

53. §

(1) Az Egyetemmel megkötött bármely szerződés tekintetében rögzíteni kell legalább az alábbiakat.
a) A kapcsolattartók adatainak megjelölésénél a következő szövegelemet kell a szerződés szövegébe beilleszteni, amennyiben az nem tartalmaz a kapcsolattartók adatvédelmére vonatkozóan előírást: „A Felek egymás kapcsolattartói adatait jogos érdekből [GDPR 6. cikk (1) bekezdés f) pontja alapján] kezelik a szerződés fennállásának teljes időtartama alatt, majd pedig a szerződés megszűnését követően a jogviszonyból esetlegesen származó jogi igények érvényesítésének határidejéig vagy a szerződéses jogviszonyra vonatkozóan előírt bizonylati megőrzési időig. A Felek kötelezettséget vállalnak arra, hogy a kapcsolattartásra megjelölt mind a saját, mind a Partner kapcsolattartóját tájékoztatják az adatkezelésről erre vonatkozó adatkezelési tájékoztató elkészítésével és közzétételével.” Az Egyetem e tárgykörű adatkezelési tájékoztató mintasablonját a JII készíti el és tartja naprakészen, valamint elérhetővé teszi az egység adatvédelmi referensei számára.
b) Amennyiben a szerződésben előírt feladat során személyes adatok kezelése valósul meg, szükséges a szerződésben rögzíteni, hogy a Felek az adatkezelésre vonatkozó mindenkori hatályos jogszabályok előírásainak betartásával járnak el.
(2) Az Egyetemmel megkötendő, adatkezelést érintő szerződések aláírására kizárólag abban az esetben kerülhet sor, ha az adatkezelés vonatkozásában a Felek adatvédelmi szerepkörét (önálló adatkezelő, közös adatkezelők, adatfeldolgozó) tisztázták, és azt a Felek a szerződésben írásba foglalták.
(3) Írásbeli megkereséssel (ideértve az elektronikus levelet is) kérelmezhető
a) a DPO-tól a szerződések adatvédelmi szempontú véleményezése, valamint
b) az információbiztonsági felelőstől a szerződések adatbiztonsági szempontú véleményezése.
A véleményezésre legalább 20 napos határidőt szükséges biztosítani mind a DPO-nak, mind az információbiztonsági felelős számára.

### *Okmánymásolás tilalma*

54. §

(1) Jelen Szabályzat hatálya alá tartozók az adatkezelési tevékenységeik során jogszabályi felhatalmazás nélkül a személyazonosító okmányokról másolatot nem készíthetnek.

(2) Amennyiben az ügymenet az elszámoltathatóság okán megköveteli, a személyazonosítás elvégzése után írásban feljegyezhető, hogy az azonosítás milyen típusú okmány alapján történt.
(3) Törekedni kell rá, hogy minden adminisztrációs ügymenet vonatkozásában az ügyintézés gyorsítása és pontossága érdekében kialakításra kerüljön egy olyan, adatbiztonság szempontjából megfelelő elektronikus felület, ahol a jogviszony létrejötte érdekében a másik fél (pl. leendő hallgató, leendő munkavállaló stb.) a folyamatra elkészített adatkezelési tájékoztató megismerését követően, előzetesen beírhatja a jogviszonyhoz szükséges és még éppen elégséges adatköreit, annak érdekében, hogy a személyes megjelenésekor az általa előzetesen az elektronikus felületen megadott személyes adatai az eredeti okmányai alapján összevetésre kerüljenek.

### *Nyilvántartási rendszerekkel szembeni adatvédelmi elvárások*

55. §

(1) A személyes adatok nyilvántartására szolgáló nyilvántartó rendszerek adatkezeléseinek is meg kell felelniük a vonatkozó adatvédelmi jogszabályoknak és az Egyetem belső szabályzóinak. A nyilvántartási rendszerekben tárolt személyes adatok kezelése során is érvényesek az adatvédelmi alapelvek és az adatvédelmi előírások, különösen a célhoz kötött adatkezelés, a pontosság, a korlátozott tárolhatóság, az adattakarékosság, valamint a tisztességesség alapelvei.
(2) Az Egyetem használatában lévő személyes adatot kezelő bármely elektronikus nyilvántartási rendszer működése abban az esetben jogszerű, ha a rendszer legalább az alábbi feltételek mindegyikét teljesíti:
a) Minden nyilvántartási rendszernek képesnek kell lennie arra, hogy az érintett személy gyakorolhassa a hozzáférés jogát, melynek keretében az érintett személyes adatai vonatkozásában elszámoltatható módon kapjon visszajelzést arra nézve, hogy személyes adatait ki és milyen jogszerű cél mentén ismerte meg (naplófile), valamint a nyilvántartott adatairól másolatot kérhessen.
b) Ha a nyilvántartási rendszert nem az Egyetem üzemelteti, akkor a rendszer üzemeltetőjével, fenntartójával, supportot nyújtó szolgáltatóval, amennyiben személyes adatok bármely köréhez ideiglenes vagy tartós jelleggel bármilyen módszerrel hozzáfér, rálát vagy egyéb módon kezel, adatfeldolgozási szerződést szükséges megkötni, kivéve az 51. § (8) bekezdésben meghatározott jogszabályi előíráson alapuló adatfeldolgozás esetkörét
c) A rendszerhez való jogosultságok kiosztása, ellenőrzése és visszavonása szabályozott eljárás mellett hatékonyan történik.
d) Megfelelő technikai és szervezési intézkedésekkel kerüljön biztosításra, hogy az adatkezelési műveletek végzése során a személyes adatokhoz kizárólag az és olyan mértékben rendelkezzen hozzáféréssel, akinek az adatkezelési művelettel összefüggő feladatának ellátáshoz feltétlenül szükséges.
(3) Amennyiben adatkezelést végző szervezeti egység (2) bekezdésben felsoroltak valamelyike tekintetében integritássértést tapasztal, köteles a DPO-nál és a JII-nál kezdeményezni az integritássértés feloldását.
(4) A (2) bekezdésben leírt elvárások teljesülését az újonnan beszerezni kívánt nyilvántartási rendszerek esetén a beszerzést koordináló központi adatkezelést végző szervezeti egység köteles ellenőrizni még a beszerzés megindítása előtt.

(5) A nyilvántartási rendszerek háttértámogatását biztosító külső személyek/szervezetek adatvédelmi megfelelőségéért, valamint az érintettek jogszerű tájékoztatásáért, továbbá az érintettek joggyakorlásának teljesítéséért az a központi adatkezelést végző szervezeti egység a felelős, amely a nyilvántartási rendszer által kezelt személyes adatokért hatáskörileg felelős.
(6) A nyilvántartási rendszerért felelős központi adatkezelést végző szervezeti egység belső eljárásrendben (pl. munkautasításban) rögzíti, hogy a nyilvántartási rendszerhez ki és milyen mértékben férhet hozzá, kezelheti jogszerűen.
(7) Az (6) bekezdésben leírt belső eljárásrend másolati példányát a szervezeti egység a DPO számára megküldi legkésőbb annak elkészítésétől számított 8 munkanapon belül. A belső eljárásrendet a szervezeti egység köteles naprakészen vezetni, és évente legalább egyszer felülvizsgálni.

56. §

(1) A különleges személyes adatok tekintetében fokozott gondossággal kell eljárni.
(2) Az egészségügyi adatok kezelésének szabályaira jelen Szabályzat mellett az egészségügyi adatkezelésre vonatkozó jogi előírások, valamint az Egyetem Egészségügyi Adatkezelési Eljárásrendje mérvadók.

### *Adatvédelmi hatásvizsgálat és előzetes hatósági konzultáció*

*[Kapcsolódó jogi háttér: GDPR (95) preambulumbekezdése, és a 35-36. cikkei]*

### *Adatvédelmi hatásvizsgálat szükségessége*

57. §

(1) Ha az adatkezelés valamely – különösen új technológiákat alkalmazó – típusa, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, akkor a központi adatkezelést végző szervezeti egység az adatkezelést megelőzően hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik (ez az ún. adatvédelmi hatásvizsgálat).
(2) Az egymáshoz hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló magas kockázatokat jelentenek, egyetlen hatásvizsgálat keretei között is értékelhetők.
(3) Az adatvédelmi hatásvizsgálatot különösen az alábbi esetekben szükséges elvégezni:
a) természetes személyekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelése, amely automatizált adatkezelésen – ideértve a profilalkotást is – alapul, és amelyre a természetes személy tekintetében joghatással bíró vagy a természetes személyt jelentős mértékben érintő döntések épülnek,
b) egészségügyi és más, a személyes adatok különleges kategóriáinak nagy számban történő kezelése esetén,
c) büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok nagy számban történő kezelése esetén,
d) nyilvános helyek nagymértékű, módszeres megfigyelése, így például az elektronikus megfigyelőrendszer (kamera) alkalmazása,
e) biometrikus azonosítás bármilyen formája,

f) azon adatkezelések esetén, amelyek az Adatvédelmi Hatóság adatvédelmi hatásvizsgálatot kötelezően előíró jegyzékében megtalálhatók,
g) a DPO által javasolt esetekben.
(4) A DPO-tól írásbeli megkeresés (ideértve az elektronikus levelet is) alapján az adatkezelést végző szervezeti egység köteles állásfoglalást kérni
a) tervezett adatkezelés magas kockázatú minősítése,
b) a tervezett automatizált adatkezelés természetes személyek jogait, szabadságait jelentős mértékben érintő minősítése,
c) az Adatvédelmi Hatóság adatvédelmi hatásvizsgálatot kötelezően előíró, illetve a hatásvizsgálat alól mentességet élvező adatkezelési jegyzéke,
d) a hatásvizsgálat elvégzésekor felmerülő adatvédelmi kérdések
tekintetében.
(5) A DPO számára a (4) bekezdés szerinti állásfoglalás elkészítésére legalább 30 napot kell biztosítani.
(6) Nem kell adatvédelmi hatásvizsgálatot lefolytatni
a) a jogszabályon alapuló adatkezelések és a jogi kötelezettség teljesítéséhez szükséges adatkezelések esetén, valamint
b) azon adatkezelések esetén, amelyek az Adatvédelmi Hatóság adatvédelmi hatásvizsgálat alól mentességet élvező adatkezelések jegyzékében találhatók.

### *Adatvédelmi hatásvizsgálat elkészítése*

58. §

(1) A hatásvizsgálat legalább az alábbi elemek mindegyikét tartalmazza:
a) a tervezett adatkezelési műveletek módszeres leírását,
b) az adatkezelés céljainak ismertetését, beleértve adott esetben az adatkezelő által érvényesíteni kívánt jogos érdeket,
c) az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatát, beleértve annak értékelését, hogy megvalósítható-e a tervezett adatkezelési cél személyes adatkezelés nélkül, illetve más, olyan módszerrel, amely az érintett magánszférájába kevésbé hatol be,
d) az érintett jogait és szabadságait érintő kockázatok vizsgálatát,
e) a kockázatok kezelését célzó intézkedések bemutatását, ideértve a személyes adatok védelmét és a GDPR-ral, valamint jelen Szabályzattal való összhang igazolását szolgáló, az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákat, biztonsági intézkedéseket és mechanizmusokat,
f) a hatásvizsgálatot elkészítő központi adatkezelést végző szervezeti egység megnevezését, vezetőjének és kapcsolattartójának nevét, munkahelyi elérhetőségét és aláírását,
g) az adatvédelmi hatásvizsgálat elkészítésének dátumát,
h) a tervezett adatkezelés megkezdésének időpontját.
(2) Az adatkezelést végző szervezeti egység adott esetben – az adatkezelési műveletek biztonságának sérelme nélkül – kikérheti az érintettek vagy képviselőik véleményét a tervezett adatkezelésről.
(3) A hallgatói adatokat érintő adatvédelmi hatásvizsgálat esetén a központi adatkezelést végző szervezeti egység kikéri az érintett hallgatók hallgatói (rész)önkormányzatának véleményét.
(4) A külső (különösen pályázati) forrásból megvalósuló olyan adatkezelések esetén, amelyeknél az adatvédelmi hatásvizsgálat elvégzése kötelező, e források terhére kell

biztosítani az adatvédelmi hatásvizsgálat elvégzését. A tervezett adatkezelést megvalósítani kívánó adatkezelést végző szervezeti egysége vagy a pályázatot előkészítő szervezeti egység a pályázat benyújtása előtt kikéri a DPO véleményét az adatvédelmi hatásvizsgálat szükségességéről.
(5) Az elkészült hatásvizsgálat eredményét a DPO-nak meg kell küldeni. A DPO a hatásvizsgálattal kapcsolatban észrevételeket tehet.
(6) Az elkészített hatásvizsgálatot a központi adatkezelést végző szervezeti egység őrzi meg
a) a meg nem valósult adatkezelések esetén az elkészítést követő 1 évig,
b) a megvalósuló adatkezelések esetén az adott adatkezelés megőrzési idejéhez igazodóan.
(7) Az adatkezelést nem lehet megkezdeni, ha az az érintettek személyiségi jogaira vagy szabadságaira nézve magas kockázatú.
(8) A központi adatkezelést végző szervezeti egység az elkészített hatásvizsgálatra köteles rávezeti:
a) az előzetes konzultáció lefolytatásának tényét és idejét, ha a Szabályzat 59. §-ában meghatározott előzetes konzultáció lefolytatására sor került.
b) a Szabályzat 60. §-ában leírt DPO ellenőrzések időpontját és megállapításait.

### *Előzetes konzultáció*

59. §

(1) Amennyiben az adatvédelmi hatásvizsgálat megállapítja, hogy a tervezett adatkezelés – a kockázatok mérséklése céljából tett intézkedések hiányában – ténylegesen magas kockázattal járna, és a hatásvizsgálatot elvégző szervezeti egység vezetője a DPO-t arról tájékoztatja, hogy a tervezett adatkezelésre vonatkozó igényt továbbra is fenntartja, a DPO az adatkezelés tervezett kezdőidőpontját legalább 14 héttel megelőzően konzultál az Adatvédelmi Hatósággal.
(2) A DPO az előzetes konzultáció során az Adatvédelmi Hatóságot különösen az alábbiakról köteles tájékoztatni a hatásvizsgálatot elvégző szervezeti egység által megadott információk alapján:
a) a tervezett adatkezelésben részt vevő adatkezelő, közös adatkezelők és adatfeldolgozókról, illetve azok feladatköreiről,
b) a tervezett adatkezelés céljairól,
c) a tervezett adatkezelésről (adatkezelés leírása),
d) az érintettek GDPR szerint fennálló jogainak és szabadságainak védelmében hozott intézkedésekről és garanciákról,
e) az adatvédelmi hatásvizsgálat elvégzéséről, és eredményéről.
(3) A DPO az előzetes konzultáció során az Adatvédelmi Hatóság részéről felmerülő kérdéseket köteles megválaszolni, valamint közvetíteni a hatásvizsgálatot elvégző szervezeti egység és az Adatvédelmi Hatóság között.

### *Adatvédelmi hatásvizsgálatnak való megfelelés ellenőrzése*

60. §

(1) Az adatvédelmi hatásvizsgálatot elkészítő szervezeti egység vezetője köteles az elkészített hatásvizsgálatot az érintett adatkezelési tevékenységeket megvalósító személyekkel megismertetni, és annak betartását megkövetelni és ellenőrizni.

(2) A DPO az adatvédelmi hatásvizsgálattal érintett adatkezelés megkezdését követően ellenőrzést végez annak értékelése céljából, hogy a személyes adatok kezelése az adatvédelmi hatásvizsgálatnak megfelelően történik-e. Ezt követően pedig szükség szerint, de legalább az adatkezelési műveletek által jelentett kockázat változása esetén folytat ellenőrzést.
(3) Az adatvédelmi hatásvizsgálatot elkészítő szervezeti egység köteles a hatásvizsgálattal érintett adatkezelésben beálló változásokat – legfeljebb a változás bekövetkezésétől számított 5 munkanapon belül – jelenteni a DPO számára. A változásbejelentés nyomán a DPO legfeljebb 15 napon belül mérlegel, hogy szükséges-e bármiféle változtatás az adatkezelési folyamatban.

### *Személyes adatok megismerhetővé tétele*

*[Kapcsolódó jogi háttér: GDPR (61), (63), (111) preambulumbekezdései, 13. cikk (1) bekezdés e) pontja, valamint a GDPR 14. cikk (1) bekezdés e) pontja, továbbá a 15. cikk (1) bekezdés c) pontja]*

61. §

(1) Az Egyetemen a személyes adatok bármilyen módon megvalósuló – ideértve a szóbeli vagy írásbeli közlést, ráutaló magatartással, illetve mulasztással beálló hozzáférhetővé tételt, nyilvánosságra hozatalt – adatátadás, adattovábbítás (továbbiakban: megismerhetővé tétel) tekintetében alkalmazni kell az adatvédelmi előírásokat.
(2) Nem minősül sem adatátadásnak, sem adattovábbításnak az érintett saját személyes adataihoz való hozzáférésének biztosítása. Az érintett saját adataihoz való hozzáférésének biztosítása tekintetében is körültekintően kell eljárni. Minden esetben a lehető legnagyobb gondossággal kell törekedni arra, hogy az érintett csak a saját adatait ismerhesse meg és az érintetten kívül más, arra jogosulatlan személy az érintett személyes adatait ne ismerhesse meg.
(3) A személyes adatok megismerhetővé tételéről saját hatáskörében az adatkezelést végző személy, illetve kérdése esetén az adott adatkezelést végző szervezeti egység vezetője dönt az adatvédelmi elvárások, különösen a célhoz kötött adatkezelés és az adattakarékosság elvének figyelembevételével. Amennyiben a jogszerűséggel kapcsolatban kétség merül fel, a szervezeti egység vezetője köteles írásban (ideértve az elektronikus levelet is) a DPO-hoz fordulni, aki állásfoglalást ad ki a tervezett adatkezelési műveletek jogszerűségéről.
(4) A személyes adatok rendszeres jellegű megismerhetővé tételéről az érintett személyeket előzetesen tájékoztatni kell. A tájékoztatás az adatvédelmi jogi előírásoknak megfelelő módon összeállított adatkezelési tájékoztató része, amely tartalmazza a személyes adatok megismerhetővé tételének formáit.
(5) A személyes adatok egyedi jellegű megismerhetővé tételéről az érintett az alábbi módokon értesül:
a) amennyiben annak jogalapja önkéntes hozzájárulás, az érintett előzetes tájékoztatáson alapuló hozzájárulásának beszerzéséért az adatkezelést végző szervezeti egység felel,
b) az érintett minden esetben tájékoztatást kérhet saját személyes adatának egyedi jellegű adatátadásáról, valamint adattovábbításáról az adatátadó, adattovábbító szervezeti egység egyedi adatátadási, illetve egyedi adattovábbítási nyilvántartásából.

62. §

(1) Személyes adatok átadása vagy továbbítása során, amennyiben az postai (akár belső, akár külső) küldeményként történik, minden esetben biztosítani kell, hogy a küldemény zárt módon kerüljön feladásra.
(2) Az egyetemi kézbesítő köteles megtagadni a nem zárt küldemények átvételét.
(3) Az egyetemi kézbesítők önálló felelősséggel tartoznak a zárt küldemények bontatlan, sérülésmentes kézbesítéséért.
(4) A személyes adatok különleges kategóriáit tértivevényes küldeményben kell postára adni, „saját kezébe (sk.)" jelzéssel. Az átvevő aláírását és a kézbesítés dátumát tartalmazó tértivevényt vagy postakönyvet az Egyetem iratkezelési szabályzatának megfelelő módon és ideig kell megőrizni.

63. §

(1) Személyes adatok elektronikus úton történő bármilyen típusú megismerhetővé tétele során ügyelni kell, hogy
a) a munkahelyi feladatok ellátásához kötődő, hivatalos ügyekben kizárólag a munkahelyi (hivatalos) e-mail címek használata a megengedett,
b) kizárólag azon személyek számára kerüljön megküldésre az adott levél (ideértve a csatolmányokat is), akik az ügyhöz szorosan hozzárendelhetők (különösen előzmény-folyamatok, illetve munkaköri feladatuk okán),
c) a levelek továbbítása („forward") megfontolandó a belső levelezések során, tekintettel az eredeti levelezés hangnemére, jellegére, ezért lehetőség szerint kerülendő, kivéve, ha erre a munkahelyi vezető tájékoztatása érdekében a vezető által elrendelt belső eljárási rend szerint kerül sor,
d) a belső munkalevelezések továbbítása („forward") az Egyetemen kívülre nem megengedett, helyette az ügy tartalmi lényegét szükséges ismertetni olyan mértékben, amelyet az adott ügy megkíván, és az eredeti levelet küldő személy e-mail címét másolati mezőben kell megadni,
e) amennyiben személyes adat kerül átadásra, továbbításra, különösen figyelni kell arra, hogy már a tárgymezőbe belekerüljön a „bizalmas információ, kizárólag a címzett részére" megjelölés.
(2) Egyebekben az Egyetem elektronikus levelezésre vonatkozó belső szabályzói, valamint az információbiztonsági szabályzatban megköveteltek mentén szükséges eljárni.

### *Adatátadás az Egyetem szervezeti rendszerén belül*

64. §

(1) Az Egyetem szervezeti rendszerén belül, az elszámoltathatóság és az átláthatóság biztosítása érdekében, személyes adatok – a feladat elvégzéséhez szükséges és elégséges mértékben és ideig – csak olyan, az adatkezelésre jogosult szervezeti egységhez, személy számára adhatók át, amelynek, illetve akinek feladata ellátásához szükséges a személyes adatok megismerése és kezelése, valamint az adatkezelésre megfelelő jogalappal rendelkezik.
(2) Az adatátadás akkor jogszerű, ha legalább a felsoroltak egyike teljesül az alábbiak közül:

a) az érintett adatkezelést végző szervezeti egységek adatkezelési tevékenységek nyilvántartásában benne van az adott adatkezelés, mint ellátandó feladat,
b) az Egyetem SZMr-je előírja az együttműködést az adott az adatkezelést végző szervezeti egységek között adott feladat, adott adatkezelés tekintetében,
c) az adott adatkezelést végző szervezeti egységek vezetői írásbeli megállapodásban rögzítik, és ezt a megállapodást jóváhagyja a megállapodást megkötő vezetők közös felettes vezetője,
d) az adott szervezeti egység vezetője a cél és jogalap megjelölésével kéri az adatátadását.
(3) A (2) bekezdés b) pontja esetén a lehető legrövidebb időn belül, legkésőbb az Egyetem SZMr-jének elfogadását követő 30 napon belül gondoskodni kell arról, hogy az adott adatkezelést végző szervezeti egységek adatkezelési tevékenységek nyilvántartásába is belekerüljön a vonatkozó adatkezelés.
(4) A (2) bekezdés c) és d) pontja esetében meg kell vizsgálni az adott adatkezelés rendszeres, tartós jellegét, valamint időszakosan felül kell vizsgálni azokat.
(5) Amennyiben a (4) bekezdés szerint az adatkezelés rendszeres, tartós jellege fennáll, haladéktalanul kezdeményezni kell az adott adatkezelés vonatkozásában az Egyetem SZMr-jének megfelelő módú kiegészítését, és az adott szervezeti egység adatkezelési tevékenységek nyilvántartásába való beintegrálást a (3) bekezdés szerinti határidővel.
(6) Amennyiben az adatkezelés ideiglenes, átmeneti jellegű, akkor ezen adatátadásokról az adatot átadó szervezeti egységnek külön nyilvántartást (egyedi adatátadás nyilvántartást) kell vezetni a 65. § szerint.
(7) A (2) bekezdés d) pontjában leírtak meglétét és helyességét a személyes adatokat átadó adatkezelést végző szervezeti egység ellenőrizni köteles.
(8) Az adatigénylést meg kell tagadni, ha az adatigénylő az adatkezelés jogszerű célját és jogalapját – felszólítás ellenére – nem, vagy hiányosan jelöli meg.
(9) A jogosulatlan adatátadás adatvédelmi incidenst eredményez.

### *Egyedi adatátadás nyilvántartás*

65. §

(1) Az egyedi adatátadás nyilvántartás kötelező elemei:
a) a személyes adatot átadó adatkezelést végző szervezeti egység neve, valamint az ügyintézésben közreműködő munkatársak nevei, beosztásai, munkahelyi elérhetőségei,
b) az adatátvevő szervezeti egység megnevezése, valamint az ügyintézésben közreműködő munkatársak nevei, beosztásai, munkahelyi elérhetőségei,
c) az adatok forrásának megnevezése,
d) az adatátadás célja,
e) az adatátadás jogalapja,
f) adatátadás időpontja,
g) az adatátadással érintett személyek kategóriája és (becsült) száma, vagy az érintett személy neve (és amennyiben elengedhetetlen a beazonosításához, az ahhoz szükséges alapparaméterek a 30. § (5) bekezdése szerint)
h) az átadott adatok köre
i) az adatátadás módszere (manuális, elektronikus, vegyes)
j) szükség esetén az alkalmazott adatbiztonsági intézkedések.
(2) A DPO a nyilvántartás meglétét és minőségét jogosult ellenőrizni.
(3) Mivel az adatátadás, a szervezeten belüli munkamegosztásra tekintettel, jogos érdeken és nem önkéntes hozzájáruláson alapul, ezért az érintett hozzájárulását az adatátadás előtt nem kell beszerezni.

(4) Az egyedi adatátadások tekintetében az informális önrendelkezés biztosítása érdekében az Egyetem, az érintett hozzáférési kérelme alapján, az érintettre vonatkozó személyes adatok egyedi adatátadásáról is informálja az érintett személyt.
(5) Az egyedi adatátadás nyilvántartás mintadokumentumát a JII feladata elkészíteni, és az adatvédelmi referensek számára elérhetővé kell tennie.

### *Vitarendezés az adatátadás során*

66. §

(1) Amennyiben az adatkezelést végző szervezeti egység és az adatokat megismerni kívánó szervezeti egység között az adott adatkezelés jogszerűsége és a feladatellátással összefüggő szükségessége, arányossága kapcsán vita merül fel, a vitát mindkét szervezeti egység tekintetében az illetékes felsővezető írásban dönti el.

(2) Amennyiben az (1) bekezdésben megjelölt vezető nincs, a feladatellátással kapcsolatos vitát – az Nftv.-ben foglalt feladatmegosztásnak megfelelően – a Rektor vagy a Kancellár írásban dönti el.

(3) A vita eldöntéséhez a felsővezető kikérheti a DPO véleményét.

67. §

Az Egyetemen folyó különböző célra irányuló, különböző jogalappal bíró adatbázisok, nyilvántartások csak törvényes céloknak megfelelően, az összekapcsolást kezdeményező által előzetesen elvégzett és a DPO által jóváhagyott érdekmérlegelés alapján, csak indokolt esetben és ideig kapcsolhatók össze.

### *Adattovábbítás*

*[Kapcsolódó jogi háttér: GDPR (31) preambulumbekezdése, 4. cikk 9. pontja]*

68. §

(1) Az Egyetem szervezeti rendszerén kívülre, az elszámoltathatóság és az átláthatóság biztosítása érdekében, személyes adatok – a feladat elvégzéséhez szükséges és még éppen elégséges mértékben és ideig – csak olyan, az adatkezelésre jogosult harmadik fél számára továbbíthatók, amelynek, illetve akinek feladata ellátásához szükséges a személyes adatok megismerése és kezelése, valamint az adatkezelésre megfelelő jogalappal rendelkezik.
(2) Az adattovábbítás akkor jogszerű, ha legalább a felsoroltak egyike teljesül az alábbiak közül:
a) az adattovábbítás jogalapja önkéntes hozzájárulás, és az érintett személy tájékoztatáson alapuló önkéntes hozzájárulása beszerzésre került,
b) az adattovábbítást végző szervezeti egység adatkezelési tevékenységek nyilvántartásában benne van az adattovábbítás, mint ellátandó feladat,
c) az adattovábbítás jogszabályon, jogi kötelezettség teljesítésén alapul,
d) az Egyetem SZMr-je előírja az adattovábbítást végző szervezet számára az adott harmadik féllel való együttműködési kötelezettséget,

e) a harmadik fél a cél és jogalap megjelölésével írásban (ideértve az elektronikus levelet is) kéri az adattovábbítást,
f) az adattovábbításban érintett szervezeti egység felettes vezetője a cél és jogalap megjelölésével írásban (ideértve az elektronikus levelet is) kéri az adattovábbítást.
(3) A (2) bekezdés a) pontja értelmében a hozzájáruláson alapuló adatkezelésekből történő adattovábbítás esetén a hozzájárulásnak kifejezetten az adattovábbításra is ki kell terjednie. Amennyiben az önkéntes hozzájárulást nem az adattovábbító szervezeti egység szerzi be, köteles a hozzájárulás meglétét és annak adattovábbításra kiterjedő tartalmát ellenőrizni.
(4) A (2) bekezdés c) pontja vonatkozásában az adattovábbításra az adott jogszabályi hely hatályának ellenőrzése után kerülhet sor.
(5) A (2) bekezdés d) pontja esetén a lehető legrövidebb időn belül, legkésőbb az Egyetem SZMr-jének elfogadását követő 30 napon belül gondoskodni kell arról, hogy az adott adatkezelést végző szervezeti egység adatkezelési tevékenységek nyilvántartásába belekerüljön a vonatkozó adatkezelés.
(6) A (2) bekezdés e) pontja tekintetében a megkereséshez kapcsolódó adatkezelési cél és jogalapjának ellenőrzése, valamint felelős megítélése azon adatkezelést végző szervezeti egység felelőssége, amely az adott megkeresés címzettje. A megkeresés adatkezelési célja és jogalapjának megítélése tekintetében a DPO véleménye írásban (ideértve az elektronikus levelet is) kikérhető.
(7) A (2) bekezdés f) pontja értelmében a helyes jogalap és jogszerű cél megjelölése a felettes vezető felelőssége, ugyanakkor az utasított szervezeti egység, személy kötelessége felhívni a felettes vezető figyelmét arra, ha jogsértést tapasztalna.
(8) A jogosulatlan adattovábbítás adatvédelmi incidenst eredményez.
(9) Az adatigénylést meg kell tagadni, ha az adatigénylő az adatkezelés jogszerű célját és jogalapját – felszólítás ellenére – nem, vagy hiányosan jelöli meg.
(10) A közhatalmi szervek, amelyek egyedi vizsgálat keretében uniós vagy nemzeti joggal összhangban kérnek információt és adattovábbítást az Egyetemtől, nem minősülnek címzettnek, ennek okán az adattovábbításról nem szükséges tájékoztatni az érintett személyt sem előzetesen, sem hozzáférési kérelme alapján. A közhatalmi szervek megkeresésein alapuló adattovábbításokról az adattovábbító szervezeti egység nem köteles egyedi nyilvántartás vezetésére.
(11) A nemzetbiztonsági szolgálatok adatkérésre irányuló megkereséseiről az érintett szervezeti egység vezetője tájékoztatja az Egyetem Rektorát és a Kancellárt. Az ilyen megkeresések ellen a Rektor vagy a Kancellár nem halasztó hatályú panasszal fordulhat az illetékes miniszterhez. A nemzetbiztonsági szolgálatoktól érkező megkeresésre, adatbetekintésre vonatkozó adatokról – ideértve a megkeresés, betekintés tényét is –, és a megtett intézkedésekről az érintett vagy más személy, szervezet nem tájékoztatható.
(12) Az adattovábbításokat időszakosan felül kell vizsgálni. Amennyiben a felülvizsgálat fényt derít arra, hogy az adott adattovábbítás rendszeres, tartós jellege fennáll, haladéktalanul kezdeményezni kell az adott adatkezelés vonatkozásában az Egyetem SZMr-jének megfelelő módú kiegészítését, és az adattovábbítást végző szervezeti egység személyes adatvagyonába való beintegrálást a (5) bekezdés szerinti határidővel.
(13) Amennyiben az adatkezelés ideiglenes, átmeneti jellegű, akkor ezen adattovábbításokról az adatot továbbító szervezeti egységnek külön nyilvántartást (egyedi adattovábbítás nyilvántartást) kell vezetni a 69. § szerint.

### *Egyedi adattovábbítás nyilvántartás*

69. §

(1) Az egyedi adattovábbítás nyilvántartás kötelező elemei:
a) a személyes adatot továbbító, adatkezelést végző szervezeti egység neve, valamint az ügyintézésben közreműködő munkatársak nevei, beosztásai, munkahelyi elérhetőségei,
b) az adatátvevő harmadik fél megnevezése, valamint az ügyintézésben közreműködő munkatársak nevei, beosztásai, munkahelyi elérhetőségei,
c) az adatok forrásának megnevezése,
d) az adattovábbítás célja,
e) az adattovábbítás jogalapja,
f) adattovábbítás időpontja,
g) az adattovábbítással érintett személyek kategóriája és (becsült) száma vagy az érintett személy neve (és amennyiben elengedhetetlen a beazonosításához, az ahhoz szükséges alapparaméterek a 30. § (5) bekezdés szerint),
h) az továbbított adatok köre,
i) az adattovábbítás módszere (manuális, elektronikus, vegyes),
j) szükség esetén az alkalmazott adatbiztonsági intézkedések.
(2) A DPO a nyilvántartás meglétét és minőségét jogosult ellenőrizni.
(3) Az egyedi adattovábbítások tekintetében az informális önrendelkezés biztosítása érdekében az Egyetem, az érintett hozzáférési kérelme alapján, az érintettre vonatkozó személyes adatok egyedi adattovábbításáról is informálja az érintett személyt, kivéve a 68. § (10)-(11) bekezdésben leírtak esetén.
(4) Az egyedi adatátadás nyilvántartás mintadokumentumát a JII feladata elkészíteni, és az adatvédelmi referensek számára elérhetővé kell tennie.

### *Vitarendezés az adattovábbítás során*

70. §

(1) Amennyiben az adatkezelést végző szervezeti egység és az adatokat megismerni kívánó harmadik fél között az adott adatkezelés jogszerűsége és a feladatellátással összefüggő szükségessége, arányossága kapcsán vita merül fel, az adatkezelést végző szervezeti egység köteles erről a vita felmerülésekor azonnal tájékoztatni felettes vezetőjét.
(2) A vita eldöntéséhez a felsővezető kikérheti a DPO véleményét.

### *Adattovábbítás a felsőoktatási információs rendszerbe*

*[Kapcsolódó jogi háttér: Nftv. 19. § (3) bekezdése, valamint 3. sz. melléklete, Nftv. Vhr. 25. § (9) bekezdése és 6. sz. melléklete]*

71. §

(1) A felsőoktatási információs rendszer keretében nyilvántartott és kezelt személyes adatok körét a mindenkori felsőoktatásról szóló törvény és annak végrehajtási rendelete rögzíti.
(2) A Rektor a felsőoktatási információs rendszer részére történő elektronikus adatközlés hitelesítésére

a) hallgatói, doktorjelölti személyi törzs tekintetében az Oktatási Igazgatóság vezetőjét,
b) alkalmazotti személyi törzs tekintetében a Humánpolitikai Igazgatóság vezetőjét jelöli ki.

### *Adattovábbítás a köznevelési információs rendszerbe*

*[Kapcsolódó jogi háttér: Nknt. 26. címe, valamint az Nknt. Vhr. I. fejezete]*

72. §

(1) A köznevelési információs rendszer keretében nyilvántartott és kezelt személyes adatok körét az Nknt. és annak végrehajtási rendelete rögzíti.
(2) Az Egyetem fenntartásában lévő köznevelési intézmények vonatkozásában előírt és jogszabályban meghatározott adatszolgáltatási kötelezettséget a köznevelési intézmény vezetője által kijelölt foglalkoztatott látja el.
(3) A köznevelési intézmény vezetője az adatszolgáltatást végző személy nevéről, beosztásáról írásban tájékoztatja a JII-t.

### *Adattovábbítás a felnőttképzési adatszolgáltatási rendszerbe*

*[Kapcsolódó jogi háttér: Fktv., különösen annak 15. §-a]*

73. §

(1) A felnőttképzési adatszolgáltatási rendszer keretében nyilvántartott és kezelt személyes adatok körét az Fktv. és annak végrehajtási rendelete rögzíti.
(2) Az Egyetem felnőttképzést folytató szervezeti egységei vonatkozásában előírt és jogszabályban meghatározott adatszolgáltatási kötelezettséget a Felnőttképző Központ vezetője által meghatározott foglalkoztatott látja el.
(3) A Felnőttképző Központ vezetője az adatszolgáltatást végző személy nevéről, beosztásáról írásban tájékoztatja a JII-t.

### *Adattovábbítás külföldre*

*[Kapcsolódó jogi háttér: GDPR (101) preambulumbekezdése, V. fejezet]*

74. §

(1) A külföldre irányuló adattovábbítás esetén az adattovábbítást végzőnek külön meg kell győződnie arról, hogy a külföldre történő adattovábbítás GDPR-ban írt feltételei fennállnak-e, különösen vizsgálandó, hogy az adattovábbítás jogszerű jogalap mentén történik-e, és az adatok megfelelő védelmi szintje az adatokat átvevő adatkezelőnél biztosított-e.
(2) Ha az adattovábbítás az Európai Gazdasági Térség valamely államába irányul, úgy a személyes adatok megfelelő szintű védelmét külön nem kell vizsgálni.
(3) A harmadik országba vagy nemzetközi szervezet részére történő adattovábbításokra kizárólag a GDPR V. fejezetében foglalt rendelkezéseknek megfelelően kerülhet sor, így különösen, ha az Európai Bizottság megállapította, hogy a harmadik ország, vagy a harmadik

ország valamely területe, vagy egy vagy több meghatározott ágazata, vagy a szóban forgó nemzetközi szervezet megfelelő védelmi szintet biztosít.
(4) A külföldre történő adattovábbításra egyebekben e Szabályzat rendelkezéseit alkalmazni kell.
(5) Amennyiben az adatkezelést végző szervezeti egység bizonytalan a harmadik országba tervezett adattovábbítás jogszerűségét illetően, az adattovábbítás előtt konzultál a DPO-val az adattovábbítás jogszerű feltételeinek fennállásáról.

### *Adattovábbítás statisztikai céllal*

75. §

(1) Statisztikai célból személyes adatokat továbbítani kizárólag a mindenkori statisztikai törvény előírásainak betartásával lehet.
(2) A fentieken túl, jelen Szabályzat hatálya alá tartozó személyek a személyes adatokat statisztikai célra kizárólag úgy adhatnak át, hogy gondoskodnak arról, hogy az adatokat természetes személyekkel ne lehessen semmilyen módon kapcsolatba hozni.

### *A személyes adatok kezelése tudományos kutatás során*

*[Kapcsolódó jogi háttér: GDPR (33) preambulumbekezdés]*

76. §

(1) Amennyiben tudományos kutatás során személyes adatok felhasználására kerül sor, a jogszabályokban és a belső szabályzatokban előírt adatvédelmi és adatbiztonsági előírások betartásáért a kutatás vezetője a felelős.
(2) Személyes adatokat tudományos kutatási célból igényelni csak írásban lefektetett kutatási terv alapján lehet, amelyet a kutatókat foglalkoztató szervezeti egységek vezetői aláírásukkal jóváhagytak.
(3) Az adatokat kezelő szervezeti egység a kért adatokat kizárólag anonimizálás vagy álnevesítés után adhatja át a kutatóknak. A természetes személyek visszaazonosítását lehetővé tevő, a kódok és a személyazonosító adatok megfeleltetését tartalmazó táblázat csak akkor adható át, amennyiben a tudományos kutatás jogalapja az érintett hozzájárulása, vagy a visszaazonosításra – hitelt érdemlően – kizárólag az érintett létfontosságú érdekében kerülhet csak sor.
(4) A kutatás vezetője köteles gondoskodni arról, hogy a kutatásban résztvevők mindegyike – ideértve a kutatásban részt vevő hallgatókat is –
a) tájékoztatást kapjon az adatvédelmi és adatbiztonsági szabályokról (kutatásvezetői oktatás), továbbá
b) ezen szabályokat a kutatás bármely rész-folyamatában teljes körűen betartsák (kutatásvezetői ellenőrzés).
(5) A kutatásvezetői oktatás megtartásáról jegyzőkönyvet kell felvenni, amelyet az oktatáson résztvevők aláírnak.
(6) A kutatásvezetői oktatás jegyzőkönyvének kötelező tartalmi elemei az alábbiak:
a) az oktatás helyszíne,
b) az oktatás időpontja,

c) az oktatást tartó személy(ek) neve és aláírása,
d) oktatáson elhangzott fontosabb megállapítások, témakörök,
e) oktatáson részt vevők neve és aláírása,
f) amennyiben az oktatást nem a kutatás vezetője tartja, úgy a kutatás vezetőjének neve és aláírása.
(7) A kutatásban való részvétel előfeltétele a kutatásvezetői oktatáson való jelenlét.
(8) A kutatás vezetője a mindenkori hatályos adatvédelmi szabályokról a DPO-tól, illetve az egészségügyi személyes adatok vonatkozásában az egészségügyi adatvédelmi tisztviselőtől, a mindenkor hatályos adatbiztonsági szabályokról pedig az információbiztonsági felelőstől kérhet tájékoztatást.
(9) A kutatásban felhasznált személyes adatok tekintetében is szükséges betartani az adatvédelmi előírásokat, különösen
a) az adatvédelmi alapelveket,
b) az adatkezelési tevékenységek, valamint az egyedi adatátadások, egyedi adattovábbításokra vonatkozó nyilvántartás vezetésére vonatkozó szabályokat,
c) adatkezelési tájékoztató elkészítésére és közzétételére vonatkozó rendelkezéseket,
d) az adatbiztonsági előírásokat.
(10) A tudományos kutatásban felhasznált személyes adatok tekintetében végzett adatkezelési tevékenység nyilvántartásához a DPO ad módszertani útmutatást.
(11) Amennyiben a kutatásban az Egyetem adatfeldolgozót vesz igénybe, úgy köteles adatfeldolgozási szerződést kötni.
(12) Amennyiben a kutatásban az Egyetem adatfeldolgozóként vesz rész, köteles az adatkezelőt figyelmeztetni, hogy adatfeldolgozási szerződés megkötése is szükséges.
(13) A kutatásokra vonatkozó etikai szabályok betartása elengedhetetlen.

### *Az Egység adatkezelési tevékenységek nyilvántartása*

77. §

(1) A személyes adatokra vonatkozó adatkezelési tevékenységek nyilvántartásának elkészítése az adott központi adatkezelést végző szervezeti egység vezetőjének feladata.
(2) Az Egység adatkezelési tevékenységek nyilvántartása mutatja meg az adatkezelést végző szervezeti egység által kezelt személyes adatok tekintetében az alábbiakat:
a) adatkezelést végző szervezeti egység megnevezését és elérhetőségét,
b) az adott munkakör megnevezését és munkaköri részfeladatok megnevezését,
c) személyes adatok körét,
d) adatkezelési céljait,
e) jogalapjait (megjelölendő a jogi kötelezettség teljesítésének jogalapja esetén az adatkezelésre feljogosító jogszabályhely is, valamint a jogos érdek jogalapja esetén az előzetesen elkészített érdekmérlegelés nyilvántartásának helye is),
f) érintettek körét és becsült számát,
g) megőrzési idejét, mint törlésre előirányzott határidőt,
h) az egyetemi nyilvántartásokban elfoglalt helyét,
i) személyes adatok címzettjeit (a rendszeres adatátadások és adattovábbítások vonatkozásában) külön kiemelve a külföldi és azon belül a harmadik országbeli címzetteket és nemzetközi szervezetek körét,
j) az adatok forrását,
k) az adatkezelésre felhatalmazott jogosultak körét,
l) automatizált döntéshozatal (ide értve a profilalkotást is) alkalmazása esetén annak tényét,

m) amennyiben az adatkezelésben adatfeldolgozó közreműködik, az adatfeldolgozó megnevezését,
n) amennyiben az adatkezelés esetén közös adatkezelésről van szó, akkor az egyes közös adatkezelést végző adatkezelők megnevezését és munkahelyi elérhetőségi adatait,
o) a végrehajtott technikai és szervezési biztonsági intézkedések általános leírását,
p) a DPO nevét és munkahelyi elérhetőségeit.
(3) A DPO módszertani segítséget nyújt az adatkezelési tevékenységek nyilvántartás elkészítéséhez.
(4) Az adatkezelési tevékenységek nyilvántartásának felülvizsgálatát
a) évente rendszeres jelleggel legalább egy alkalommal kell elvégezni,
b) időszakos jelleggel a személyes adatvagyonfelmérésre kiható körülmény megváltozása esetén kell elvégezni, így különösen a szervezeti egység feladat- és hatásköreinek módosulása, a szervezeti egységekkel kapcsolatos egyéb változások (átszervezések) alkalmával vagy az adatkezelés alapvető körülményeinek megváltozása esetén
és jegyzőkönyvben dokumentálni a felülvizsgálat idejét, módját és eredményét.
(5) A DPO ellenőrizheti az adatkezelési tevékenységek nyilvántartásának meglétét és minőségét.
(6) Az adatkezelési tevékenységek nyilvántartását verziószámmal szükséges ellátni. Az előző verziószámmal rendelkező felmérést az adatkezelést végző szervezeti egység 5 évig köteles megőrizni, a módosítás alapjául szolgáló ok megjelölésével együttesen.
(7) Az elkészített adatkezelési tevékenységek nyilvántartását a központi adatkezelést végző szervezeti egység vezetője aláírásával 2 példányban hitelesíti. Az egyik hitelesített példányt az adatkezelést végző szervezeti egység vezetője, másik példányát a JII őrzi.
(8) Az adatkezelést végző szervezeti egységre vonatkozó adatkezelési tevékenységek nyilvántartása összhangban kell, hogy álljon az Egyetem SZMr-jével.

## III. ADATBIZTONSÁGI RENDSZABÁLYOK

*[Kapcsolódó jogi háttér: GDPR (39) preambulumbekezdés utolsó fordulata, valamint (49) preambulumbekezdés, továbbá 32. cikk]*

78. §

(1) A Kancellár és a Rektor együttesen információbiztonsági felelőst nevez ki, aki ellátja az Egyetem teljes hatókörére nézve az adatbiztonság felügyeletét, függetlenül attól, hogy e tevékenységben az Egyetem adatkezelőként vagy adatfeldolgozói minőségében vesz részt, továbbá, hogy az adatkezelés teljesen vagy részben automatizált módon, informatikai eszközzel vagy manuális módon, papíralapon történik.
(2) Az információbiztonsági felelős független, szakmai tevékenységéért közvetlenül a Kancellárnak felel.
(3) Információbiztonsági felelős pozíciója összeférhetetlen bármely olyan munkakörrel, megbízással, amelynek keretében – a jogviszony jellegétől függetlenül – a foglalkoztatott, szerződéses fél rendszerüzemeltetésért, vagyon-és személyvédelemért, iktatásért, irattárolásért, iratgondozásért felel.
(4) Az információbiztonsági felelősről részletesebben az információbiztonság témakörében, a Szenátus által jóváhagyott szabályzat rendelkezik, figyelemmel jelen Szabályzatban az adatbiztonságra, valamint az információbiztonsági felelősre előírt rendelkezésekre.

79. §

(1) Az Egyetem az információbiztonsági felelős véleményének figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítása céljából, hogy valamennyi személyes adat megfelelő szintű biztonságát garantálja, ideértve különösen
a) a személyes adatok kezelésére használt rendszerek és szolgáltatások bizalmas jellegének biztosítását, integritását, folyamatos rendelkezésre állását, valamint
b) egy incidens esetén a személyes adatokhoz való jogosulatlan hozzáférés azonnali megakadályozását és az adatok rendelkezésre állásának kellő időben történő visszaállítását.
(2) A konkrét adatbiztonsági intézkedéseket az Egyetem a tudomány és technológia mindenkori állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével az információbiztonsági felelős javaslata alapján választja meg.
(3) Több lehetséges adatbiztonsági megoldás közül azt kell választani, amely a személyes adatok és ezáltal az érintettek magánszférájának magasabb szintű, nagyobb fokú védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene az Egyetemnek.
(4) A biztonság megfelelő szintjének meghatározásakor kifejezetten és széleskörűen figyelembe kell venni az adatkezelésből eredő olyan kockázatokat, amelyek különösen a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésből erednek.
(5) A személyes adatokat védeni kell, különösen
a) a jogosulatlan
aa) hozzáférés,
ab) megváltoztatás,
ac) továbbítás,
ad) nyilvánosságra hozatal,
ae) törlés,
af) megsemmisítés, valamint
b) a véletlen megsemmisülés és sérülés, továbbá
c) az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás
ellen.
(6) Az adatbiztonsági rendszabályok érvényesítése érdekében a szükséges intézkedéseket meg kell tenni mind a manuálisan kezelt, mind a számítógépen (ideértve más elektronikus információhordozót is) tárolt és feldolgozott személyes adatok biztonsága érdekében.

80. §

(1) Az adatbiztonság érdekében az Egyetemen használt bármely elektronikus rendszerekhez való jogosultság-kiosztás szabályait írásban kell rögzíteni.
(2) A jogszerűen megigényelt jogosultságokat a lehető leggyorsabban, legkésőbb az igény beérkezésétől számított 8 munkanapon belül biztosítani kell.
(3) A jogosultságok megszűnésekor a jogosultságokat vissza kell vonni, ha lehetőség van rá, akkor automatikusan, vagy az erre irányuló igény beérkezésétől számítva a lehető leggyorsabban, legkésőbb az igény beérkezésétől számított 3 munkanapon belül.
(4) Az Egyetemen használt akár meglévő, akár újonnan bevezetni kívánt, használni tervezett bármilyen elektronikus rendszer adatbiztonsági megfelelőségéről az adott adatkezelést végző szervezeti egységnek rendelkeznie kell az információbiztonsági felelős jóváhagyásával.

(5) A központi adatkezelést végző szervezeti egységek kötelesek bejelentést tenni az információbiztonsági felelős felé
a) jelen Szabályzat elfogadását követő 60 napon belül, hogy milyen elektronikus rendszert működtetnek jelenleg, illetve
b) az új elektronikus rendszerek esetén a tervezett beszerzést megelőző legalább 30 nappal.
(6) Az (5) bekezdésben írt bejelentést az információbiztonsági felelős
a) a már működő rendszerek vonatkozásában, a bejelentések hozzá történő beérkezésének sorrendjében, az adott bejelentést követő 40 napon belül,
b) az újonnan beszerezni kívánt rendszerek vonatkozásában 30 napon belül köteles megvizsgálni, hogy megfelel-e az adatbiztonsági előírásoknak.
(7) Az információbiztonsági felelős javaslatainak figyelembevételével kell a már meglévő rendszereket működtetni és az új rendszereket beszerezni és működtetni.

### *Adatvédelmi incidens*

*[Kapcsolódó jogi háttér: GDPR 33-34. cikkei]*

### *Adatvédelmi incidens észlelése*

81. §

(1) Amennyiben az Egyetem bármely munkatársa vagy bármely érintettje adatvédelmi incidens gyanúját észleli, vagy az adatfeldolgozótól adatvédelmi incidensre vonatkozó jelzést kap, haladéktalanul értesíti az adott központi adatkezelést végző szervezeti egység adatvédelmi referensét. Az adatvédelmi incidens-gyanú észlelésekor az adott központi adatkezelést végző szervezeti egység vezetője az egysége adatvédelmi referensével együttesen haladéktalanul, legkésőbb 1 munkanapon belül megvizsgálja az eset körülményeit.
(2) Amennyiben bebizonyosodik, hogy a gyanú vélhetően incidens**,** az adott központi adatkezelést végző szervezeti egység haladéktalanul, de legkésőbb a kivizsgálási idő elteltét követően azonnal, írásban (ideértve az elektronikus levelet is) jelzi a DPO felé.
(3) A DPO a bejelentés valamennyi releváns körülményét kivizsgálja, és amennyiben incidensnek minősíti a bejelentett eseményt, haladéktalanul egyidejűleg értesíti
a) az információbiztonsági felelőst és
b) az adott központi adatkezelést végző szervezeti egység vezetőjét, valamint
c) a Kancellárt, továbbá
d) a JII vezetőjét
úgy, hogy az eset körülményeinek figyelembe vételével javaslatot fogalmaz meg az Adatvédelmi Hatóság felé történő bejelentésre vonatkozóan, valamint az érintettek tájékoztatására nézve (ún. adatkezelői tudomásszerzés az adatvédelmi incidensről).
(4) Amennyiben az adatvédelmi incidens gyanúját nem az adatkezelést végző szervezeti egység észleli, hanem más szervezeti egység vagy harmadik fél, akkor az adatvédelmi incidens gyanúját a DPO felé szükséges jelezni. A DPO a hozzá beérkező jelzést követően megkezdi a (3) bekezdésben rögzített eljárását.

### *Döntés és intézkedés*

82. §

(1) A DPO adatvédelmi incidensről szóló írásbeli tájékoztatása (ideértve az elektronikus levelet is) alapján a Kancellár a JII, valamint az információbiztonsági felelős bevonásával haladéktalanul gondoskodik
a) a megsérült, módosult vagy megsemmisült adat helyreállításáról, kijavításáról vagy pótlásáról, amennyiben az adat kezelését jogszabály írja elő, vagy az adatkezelés feltételei változatlanul fennállnak, illetve
b) a jogosulatlan hozzáférés lehetőségének megszüntetéséről.
(2) Az adatvédelmi incidens bejelentésére, valamint az érintettek tájékoztatására vonatkozó döntést – a JII javaslatai alapján – a Kancellár hozza meg. Erről írásban haladéktalanul értesíti a DPO-t.

### *Érintettek tájékoztatása*

83. §

(1) Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár az érintettet megillető valamely alapvető jog érvényesülésére, valamint magánszférájának lényeges sérülésével, továbbá az emberi méltóságát sértő következményekkel jár, illetve járhat, az adatvédelmi incidenssel érintett központi adatkezelést végző szervezeti egység vezetője az érintettet az adatvédelmi incidensről haladéktalanul tájékoztatja.
(2) A Kancellár írásbeli döntése szerinti szükséges érintetti tájékoztatást a JII készíti elő a központi adatkezelést végző szervezeti egység vezetője számára. Amennyiben az érintett az Egyetem munkatársa, és az szükséges, az érintett levelezési címét a JII kikérheti a humánpolitikai nyilvántartásból.
(3) Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell legalább a következő információkat és intézkedéseket:
a) a DPO vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és munkahelyi elérhetőségeit,
b) az adatvédelmi incidensből eredő, valószínűsíthető következményeket,
c) az Egyetem által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.
(4) Az érintettet nem kell tájékoztatni, ha a következő feltételek bármelyike teljesül:
a) az Egyetem az adatvédelmi incidenssel érintett személyes adatok tekintetében az adatvédelmi incidensről való tudomásszerzést követően azonnal megfelelő – így különösen az adatokat a jogosulatlan személy általi hozzáférés esetére értelmezhetetlenné alakító, azok titkosítását eredményező – technikaii és szervezési védelmi intézkedéseket alkalmazott,
b) az Egyetem az adatvédelmi incidensről való tudomásszerzését követően olyan intézkedéseket tett, amelyek biztosítják, hogy az adatvédelmi incidens folytán az érintettet megillető valamely alapvető jog érvényesülését lényegesen befolyásoló következmények valószínűsíthetően nem következnek be,
c) az érintett közvetlen tájékoztatása kizárólag az adatkezelő aránytalan erőfeszítésével lenne teljesíthető, ezért az adatkezelő az érintettek részére az adatvédelmi incidenssel összefüggő megfelelő tájékoztatást bárki által hozzáférhető módon közzétett információk útján biztosítja,
d) amennyiben jogszabályi előírás a tájékoztatást kizárja.

### *Adatvédelmi incidens bejelentése*

84. §

(1) Az adatvédelmi incidenst haladéktalanul, de legfeljebb az adatvédelmi incidensről való adatkezelői tudomásszerzését követő 72 órával szükséges bejelenti a Hatóságnak, ha valószínűsíthető, hogy az kockázattal jár az érintettek jogainak érvényesülésére.
(2) Az adatvédelmi incidens bejelentését a DPO végzi el a Kancellári döntésnek megfelelően, az arról szóló írásbeli tájékoztatást követően haladéktalanul.
(3) A bejelentést az Adatvédelmi Hatóság online felületén szükséges megtenni. Amennyiben az technikai okok miatt nem elérhető, akkor vagy elektronikus levélben vagy postai úton, írásban kell az Adatvédelmi Hatóságot tájékoztatni.
(4) Amennyiben a bejelentés az Adatvédelmi Hatóság online felületén keresztül történik, a Hatóság által megjelöltekre szükséges válaszolnia a DPO-nak.
(5) Amennyiben a bejelentés csupán elektronikus levél útján vagy postai úton tehető meg, ebben az esetben a megküldött bejelentés tartalmazza az alábbiakat:
a) adatkezelő nevét, címét, intézményi azonosítóját, adószámát, tevékenységi szektor besorolását,
b) a DPO nevét, telefonszámát, e-mail címét, aki egyben az adatkezelő vonatkozó bejelentés tekintetében kijelölt kapcsolattartója is,
c) az incidenssel érintett adatkezelést végző szervezeti egység megnevezését,
d) az adatvédelmi incidens időpontját,
e) az adatkezelői tudomásszerzés időpontját,
f) amennyiben az incidensről adatfeldolgozó értesítette az Egyetemet, akkor az értesítés időpontját,
g) az adatvédelmi incidens postára adás napját, mint a bejelentés időpontját,
h) az adatvédelmi incidens rövid leírását,
i) az adatvédelmi incidens jellegét,
j) az adatvédelmi incidens okait,
k) az érintettek körét és hozzávetőleges számát,
l) az incidenssel érintett adatok körét és hozzávetőleges mennyiségét,
m) az adatvédelmi incidensből eredő következmények leírását,
n) az adatvédelmi incidens előtt alkalmazott intézkedések bemutatását,
o) az Egyetem által az adatvédelmi incidens kezelésére megtett, illetve tervezett – az adatvédelmi incidensből eredő esetleges hátrányos következmények mérséklését célzó és egyéb – intézkedéseket,
p) annak tényét, hogy szükség volt-e az érintettek tájékoztatására, és amennyiben igen, akkor a tájékoztatás tervezett vagy megvalósított időpontját,
q) az ügyben esetlegesen érintett más EU-s felügyeleti szerv megnevezését.
(6) A megtett bejelentésről a DPO írásban (ideértve az elektronikus levelet is) egyidejűleg tájékoztatja
a) az információbiztonsági felelőst és
b) az adatvédelmi incidenssel érintett központi adatkezelést végző szervezeti egység vezetőjét, valamint
c) a Kancellárt, továbbá
d) a JII vezetőjét.

### *Adatvédelmi incidens-nyilvántartás*

85. §

A DPO valamennyi adatvédelmi incidensről – akár bejelentésköteles, akár nem bejelentésköteles – nyilvántartást vezet. Ezen nyilvántartás része a megtett adatkezelői intézkedések is.

### *Intézkedési terv összeállítása*

86. §

(1) Annak az adatkezelést végző szervezeti egységnek a vezetője, ahol az adatvédelmi incidens megtörtént, a DPO-val együtt intézkedési tervet készít arra nézve, hogy a jövőben hasonló incidens ne következhessen be.
(2) Az intézkedési tervet mind a bejelentésköteles, mind a nem bejelentésköteles adatvédelmi incidensek esetén is el kell készíteni az adatkezelői tudomásszerzést követő 20 munkanapon belül.
(3) Az intézkedési terv elkészítésébe más adatkezelést végző szervezeti egység is bevonható, amennyiben a jövőben hasonló jellegű adatvédelmi incidens az adott adatkezelést végző szervezeti egység együttműködésével részben vagy teljesen elkerülhető lenne.
(4) Az intézkedési terv szükségszerű elemei az alábbiak:
a) az adott adatkezelést végző szervezeti egység,
b) a DPO neve, valamint az egészségügyi adatok érintettsége esetén az egészségügyi adatvédelmi tisztviselő neve is,
c) az adatvédelmi incidens időpontja,
d) az adatvédelmi incidens jellege, rövid leírása,
e) azon okok, körülmények leírása, amelyek az incidens bekövetkezéséhez vezettek,
f) reparáló, megelőző intézkedések leírása felelősök és határidők megjelölésével,
g) az adott szervezeti egység vezetőjének, adatvédelmi referensének, adatvédelmi tisztviselő – amennyiben releváns, akkor az egészségügyi adatvédelmi tisztviselő – aláírása.
(5) Az intézkedési terv (4) bekezdés a)-e) pontokban leírtakat a DPO készíti elő az adatvédelmi incidens-nyilvántartás alapján.
(6) Az elkészült és aláírt intézkedési tervet a Kancellár részére kell megküldeni jóváhagyásra, és annak elrendelésére.
(7) Az intézkedési tervben megjelölt intézkedésekről – a Kancellári elrendelésre hivatkozással – a kijelölt felelősöket, a határidők megjelölésével haladéktalanul írásban (ideértve az elektronikus levelet is) tájékoztatja az adatkezelést végző szervezeti egység vezetője.
(8) Az intézkedési tervben foglalt feladatok megvalósulását a DPO ellenőrzi, az intézkedési tervben megjelölt valamennyi határidő leteltét követően haladéktalanul, legkésőbb 14 munkanapon belül. Az ellenőrzésről a DPO jegyzőkönyvet vesz fel. A jegyzőkönyv egy példányát eljuttatja az adott szervezeti egység vezetője, valamint a Kancellár számára, a szükséges további intézkedések megtétele érdekében. A jegyzőkönyv az adatvédelmi nyilvántartás részét képezi.

## IV. AZ ADATVÉDELEM FELELŐSSÉGI RENDSZERE

### *Kancellár feladata*

*[Kapcsolódó jogi háttér: GDPR 38. cikke]*

87. §

(1) A Kancellár közvetlen vezetése alá tartozik az adatvédelem és az adatbiztonság koordinálása az Egyetem vonatkozásában. Így mind a DPO, mind az információbiztonsági felelős közvetlenül a Kancellárnak tartozik felelősséggel.
(2) A Kancellár köteles a DPO által megtett javaslatokat megvizsgálni és megfontolni.
(3) A Kancellár köteles gondoskodni arról, hogy
a) a DPO megfelelő időben és megfelelő módon kerüljön bevonásra valamennyi, a személyes adatok védelmét érintő döntés előkészítésébe,
b) a DPO számára rendelkezésre álljon mindazon feltétel, jogosultság, erőforrás, valamint információ, amelyek a DPO által ellátandó feladatok végrehajtásához szükségesek,
c) a DPO szakértői szintű ismereteinek fenntartásához szükséges továbbképzésen egyetemi finanszírozással részt vehessen,
d) a DPO függetlensége garantálható legyen.
(4) Az egészségügyi adatvédelmi tisztviselő vonatkozásában az (1)-(3) bekezdésekben a DPO-ra vonatkozó szabályok alkalmazandók azzal az eltéréssel, hogy a Kancellár megnevezés alatt a KK elnökét kell érteni.

### *Központi adatkezelést végző szervezeti egység vezetőjének felelőssége*

88. §

(1) Az adott központi adatkezelést végző szervezeti egység vezetője felel a hozzá tartozó szervezeti egységei adatkezeléseinek jogi megfelelőségéért – különösen az adatkezelések célhoz kötöttsége, adattakarékossága és a megőrzési idők megtartása tekintetében.
(2) Ennek érdekében időszakos jelleggel minden központi adatkezelést végző szervezeti egység vezetője köteles felülvizsgálni a szervezeti egységéhez tartozó adatkezelési munkafolyamatokat, és a felülvizsgálatról jegyzőkönyvet felvenni.
(3) A felülvizsgálati jegyzőkönyv különösen az alábbiakat tartalmazza:
a) a felülvizsgálat időpontját,
b) a felülvizsgálattal érintett adatkörök, munkafolyamatok, szervezeti alegységek körét,
c) felülvizsgálat eredményét,
d) elrendelt intézkedéseket.
(4) A központi adatkezelést végző szervezeti egység vezetője felelős az adatvédelemmel kapcsolatos jogszabályi előírások és a vonatkozó egyetemi szabályzók – így különösen jelen Szabályzat – rendelkezéseinek Egységen belüli kihirdetéséért, a bennük megfogalmazott szabályok betartatásáért, és ennek érdekében az adott szervezeti egység adatkezelési tevékenységének folyamatosan ellenőrzéséért a felelősségi körébe tartozó szervezeti egységei vonatkozásában.
(5) A központi adatkezelést végző szervezeti egység vezetője a Szabályzat hatályba lépését követő 1 éven belül, azt követően legalább 3 évente szervezeti adatvédelmi ellenőrzés formájában megvizsgálja az Adatvédelmi Rend előírásainak alkalmazását, betartását. A

központi adatkezelést végző szervezeti egység vezetője a szervezeti adatvédelmi ellenőrzés lefolytatásában kérheti a DPO szakmai támogatását.
(6) A központi adatkezelést végző szervezeti egység vezetője a szervezeti adatvédelmi ellenőrzésről jegyzőkönyvet készít, és az ellenőrzés keretében feltárt adatvédelmi integritássértést a DPO-val közösen kiértékeli, valamint korrekciós intézkedési tervet készít. Az így létrejövő intézkedési terv végrehajtásáért a központi adatkezelést végző szervezeti egység vezetője felel. A DPO a folyamatot ellenőrizheti.
(7) A központi adatkezelést végző szervezeti egység adatvédelmi referenst és helyettest bíz meg. A központi adatkezelést végző szervezeti egység vezetője jogosult – a szervezeti egységei számára, létszámára, általuk kezelt személyes adataik jellegére, mennyiségére tekintettel – több adatvédelmi referenst és helyettest kinevezni, akár adatkezelési tevékenységi típushoz igazodóan is. A referensi kijelölésre az erre rendszeresített nyomtatványon kerülhet sor. A nyomtatvány elkészítése és naprakészen tartása a JII feladata.
(8) A központi adatkezelést végző szervezeti egység vezetője köteles a DPO-hoz fordulni, ha a személyes adatok kezeléséhez kapcsolódó bármely ügy megoldásában, észrevétel megválaszolásában bizonytalan, tekintettel különösen jelen Szabályzat 21. §-ában rögzítettekre.
(9) Egyéb adatvédelmi feladatukat a Szabályzat más részeiben, témaspecifikusan rögzíti.

### *Helyi adatkezelést végző szervezeti egység vezetőjének felelőssége*

89. §

(1) A helyi adatkezelést végző szervezeti egység vezetője gondoskodik arról, hogy az elfogadásra került Adatvédelmi Rendet a szervezeti egységének valamennyi munkatársa megismerje, megértse és a mindennapi tevékenységében alkalmazza.
(2) Minden adatkezelést végző szervezeti egység vezetője gondoskodik arról, hogy a szervezeti egység a hatáskörébe tartozó feladatellátása vonatkozásában
a) együttműködjön a feladatellátásához kapcsolódó horizontális adatkezelést végző szervezeti egységekkel, valamint
b) a hatékony adatvédelmi megfelelés kialakítása érdekében javaslatot fogalmazzon meg a felettes adatkezelést végző szervezeti egység vezetője számára, amennyiben úgy látja, hogy jelen Szabályzatban meghatározott adatvédelmi kötelezettségek hatékonyabban felső szintről teljesíthetők, ezen megfelelés kialakítása érdekében minden együttműködést szükséges a felettes adatkezelést végző szervezeti egység részére megadni. A DPO szakmai véleménye kikérhető.
(3) Az adott adatkezelést végző szervezeti egység vezetője jogszabálysértés észlelése esetén haladéktalanul intézkedik annak megszüntetéséről.
(4) Egyéb adatvédelmi feladatukat a Szabályzat más részeiben, témaspecifikusan rögzíti.

### *Adatvédelmi referensek feladata*

90. §

(1) Az adatvédelmi referens és helyettese az adott központi adatkezelést végző szervezeti egység vezetőjére háruló adatvédelmi feladatok koordinációját végzi az adott központi adatkezelést végző szervezeti egység vonatkozásában. Az adatvédelmi referens összekötő pont adatvédelmi ügyekben az adott központi adatkezelést végző szervezeti egységhez tartozó adatkezelést végző valamennyi munkatárs és a szervezeti egység vezetője, valamint a DPO, illetve a JII között.

(2) Az adatvédelmi referens és annak helyettese az alábbi feladatokat látja el
a) az adatkezelő szervezet vezetője és valamennyi munkatársa felé közvetíti a DPO, illetve a JII által – személyes egyeztetéseken, a referensi értekezleteken, vagy írásban (ideértve az elektronikus levelet, belső egyetemi munkafelületet is) – megosztott adatvédelmi információkat,
b) részt vesz a DPO és a JII által szervezett referensi értekezleteken,
c) továbbítja a DPO felé a központi adatkezelést végző szervezeti egységének adatvédelmi nehézségeit, kérdéseit, észrevételeit,
d) segítséget nyújt a központi adatkezelést végző szervezeti egység vezetőjének az egység adatvédelmi megfelelőségének kialakításában,
e) rendszeresen figyeli a JII által üzemeltetett belső egyetemi munkafelületet,
f) felügyeli és ellenőrzi a központi adatkezelést végző szervezeti egységen belül a DPO véleménye alapján a JII által jóváhagyott formanyomtatványok, mintasablonok használatát.
(3) Olyan személy nevezhető ki adatvédelmi referensnek, illetve helyettesének, aki
a) büntetlen előéletű,
b) teljes idejű jogviszonnyal rendelkezik az adott szervezeti egységgel,
c) képes átlátni az adott adatkezelést végző szervezeti egység egészének működését, az egyes munkavállalók feladatkörét és felelősségét,
d) rendelkezik felelősséggel és közvetlen ráhatással, a DPO útmutatásai alapján, a jogszerű adatkezelési gyakorlat kialakítására az adott adatkezelést végző szervezeti egység vonatkozásában,
e) képes együttműködni a DPO-val, valamint a JII-vel.
(4) Az adatvédelmi referenst és helyettesét nem érheti semmilyen hátrány a szervezeti egységnél feltárt adatvédelmi integritássértésre történő figyelemfelhívás, jelzés tekintetében.
(5) Az adatvédelmi referens és helyettese e feladatkörében eljárva a központi szervezeti egységén belül független, csupán a központi szervezeti egység vezetője felé tartozik felelősséggel.

91. §

Amennyiben az adott adatkezelést végző szervezeti egység vezetője vagy annak bármelyik munkatársa nem az Adatvédelmi Rend értelmében, vagy nem a DPO javaslata szerint jár el, akkor ennek jogkövetkezményei kizárólag őt terhelik.

### *A Szabályzat hatálya alá tartozó személyek felelőssége*

92. §

(1) A jelen Szabályzat személyi hatálya alá tartozó minden személy, aki munkaköréből vagy tisztségéből, megbízatásából fakadó jogok gyakorlása vagy kötelezettségek teljesítése kapcsán személyes adatba betekintést nyer, annak birtokába jut, személyes adatot megismer, feldolgoz, vagy bármilyen egyéb módon kezel – függetlenül azok jogalapjától vagy formájától – köteles
a) az adatvédelmi és az adatbiztonsági előírásokat megismerni és azoknak megfelelően kezelni és védeni a személyes adatokat,
b) a személyes adatokat kizárólag a munkaköréhez, tisztségéhez, megbízatásához közvetlenül kapcsolódó, jogszerű célra használni és köteles azokat bizalmasan kezelni, valamint saját hatáskörén belül megóvni a személyes adatokat az illetéktelen hozzáférés bármilyen formájától,

c) a tudomására jutott személyes adatok, információk tekintetében titoktartási kötelezettségét megtartani mind a jogviszony fennállása, mind annak megszűnését követően is.
(2) Adatkezeléssel járó munkakörben csak az foglalkoztatható, aki titoktartási nyilatkozatot tett.
(3) Az Egyetemmel jogviszonyban álló bármely személy jogosult közvetlenül is a DPO-hoz fordulni a fenti célok megvalósulása érdekében és észrevételt tenni, kérdést feltenni.
(4) Az Egyetemmel jogviszonyban állók felelősséggel tartoznak minden olyan kárért, amely jelen Szabályzat rendelkezéseinek be nem tartásából, illetve titoktartási kötelezettségük megszegéséből származik. Ugyanakkor minden adatkezelést végző személy csak annyiban vonható felelősségre, amennyiben rajta álló ok miatt került sor az adatvédelmi integritássértésre. Más személy vagy szervezeti egység mulasztása alapján beálló integritássértésekért, károkért kizárólag a mulasztó felet terheli az integritássértésből beálló következmények viselése iránti felelősség, illetve a károk megtérítési kötelezettsége.
(5) Jelen Szabályzat hatálya alá tartozó valamennyi személy saját maga felel azért, hogy a tevékenységének adatkezelési célját, jogalapját, megőrzési idejét – különösen felettese, illetve a DPO felhívása esetén – igazolja.
(6) Szigorúan tilos
a) a jogszerű adatkezelési céltól eltérő adatkezelés, valamint
b) a jogszerű adatkezelési céltól eltérő adatkezelésre utasítani, felbujtani, vagy annak megvalósításához segítséget nyújtani.
(7) Az adatvédelmi szabályok – különösen jelen Szabályzatban leírtak – be nem tartása munkáltatói intézkedést von maga után.
(8) Az Egyetem valamennyi foglalkoztatottja köteles írásban (ideértve az elektronikus levelet is) jelezni a közvetlen munkahelyi vezetőjének, ha olyan adatvédelmi integritássértést észlel saját feladatellátásán belül, amelynek elhárítása részben vagy egészben más személy vagy más szervezeti egység közreműködését igényelné.
(9) A közvetlen munkahelyi vezető a hozzá beérkező (8) bekezdés szerinti jelzéseket a lehető leggyorsabban köteles megvizsgálni és intézkedést kezdeményezni az integritássértés feloldása tekintetében (ideértve a jelzéssel érintett másik szervezeti egység megkeresését is).
(10) A közvetlen munkahelyi vezető köteles írásban (ideértve az elektronikus levelet is) visszajelzést tenni a munkavállaló számára a megtett intézkedésekről a hozzá beérkező jelzést követő legkésőbb 30 napon belül.
(11) A beérkező jelzéseket és azok kapcsán megtett intézkedéseket a közvetlen munkahelyi vezető nyilvántartja az integritássértés teljeskörű feloldását követő 1 évig. Ezt a nyilvántartást a DPO és a JII ellenőrizheti.
(12) Amennyiben a munkavállaló nem kap érdemi visszajelzést a közvetlen munkahelyi vezetőjétől, vagy a közvetlen munkahelyi vezető nem kap érdemi visszajelzést a jelzéssel érintett másik munkavállalótól vagy szervezeti egységtől, köteles a DPO felé jelzéssel élni az integritássértés tekintetében.
(13) A DPO a (12) bekezdés szerinti jelzés nyomán felhívja az érintett munkavállaló, illetve szervezeti egység figyelmét 8 napos határidő kitűzésével a szükséges visszajelzés megtételére.
(14) Amennyiben a (13) bekezdés szerinti határidő is eredménytelenül telik el, a DPO köteles az adatvédelmi integritássértést jelezni a Kancellár felé, aki a (7) bekezdés szerinti munkáltatói intézkedés mellett megteszi a szükséges intézkedést az integritássértés feloldása érdekében. Az elrendelt munkáltatói intézkedésről, valamint a szükséges intézkedések elrendeléséről tájékoztatja a JII-t, aki informálja a (12) bekezdés szerinti bejelentőt ezekről.
(15) A JII a DPO felé jelzett integritássértési ügyekről nyilvántartást vezet.

93. §

(1) Az egyetemi rendszerek bármelyikéhez jogosultsággal rendelkező személy önálló felelősséggel rendelkezik, hogy az adott rendszerhez tartozó azonosítóját és jelszavát biztonságosan kezelje.
(2) A hozzáférést biztosító jelszót, azonosítót más személy számára tilos – akár ideiglenesen, akár állandó jelleggel – átadni, hozzáférhetővé, illetve bármilyen módon megismerhetővé tenni.
(3) Amennyiben az adott rendszer használatára jogosult felhasználó észleli, hogy az azonosítójával, a jelszavával más személy bármilyen formában visszaélt, annak gyanúja, vagy akár annak érdemi lehetősége felmerült, köteles azt haladéktalanul jelezni a szervezeti egységének vezetője és a központi adatkezelést végző szervezeti egységének adatvédelmi referense felé. A jelzést a szervezeti egység vezetője és az adatvédelmi referens azonnal megvizsgálja, a bejelentést dokumentálja, és megteszi a szükséges intézkedéseket a DPO bevonásával.
(4) Az adatvédelmi szabályok vétkes megszegése, gondatlanság vagy szándékos adatvédelmi incidens előidézése esetén munkáltatói intézkedésnek lehet helye, amelyről a munkáltatói jogokat gyakorló vezető dönt, megismerve a szabályszegés vagy az incidens körülményeit és a DPO vizsgálatának eredményét.
(5) A dolgozó vétkessége okozta joghátrányt a munkáltató a Munka Törvénykönyvének vonatkozó szabályai alapján részben vagy egészben a munkavállalóra áthárithatja.
(6) A munkáltatói intézkedésnek előítéletektől és megkülönböztetéstől mentesnek, tisztességesnek és arányosnak kell lennie, betartva a fokozatosság elvét.
(7) Amennyiben a munkavállaló a munkaköri kötelezettségét gondatlansága miatt megszegi, a hibáját elismeri és megtesz minden tőle telhetőt a következmények elhárítására, valamint az Egyetemet más joghátrány nem éri, akkor a munkáltató az adatvédelmi képzés ismételt elvégzésére kötelezheti a munkavállalót.
(8) Ismételt jogsértés esetén a munkáltató először szóbeli, azt követően pedig írásbeli figyelmeztetésben részesítheti az adatvédelmi szabályokat gondatlanságból megszegő munkavállalót.
(9) Kirívóan súlyos esetben, szándékos incidens okozása esetén a dolgozó azonnali elbocsátása és az okozott kár megtérítésére kötelezés lehet a szankció.
(10) A munkáltatói döntéssel szemben a munkavállaló jogorvoslattal élhet.

### *Az adatvédelmi tisztviselő*

*[Kapcsolódó jogi háttér: GDPR 37-39. cikkei]*

#### *Kinevezése*

94. §

(1) Az Egyetem a személyes adatok kezelésére vonatkozó jogi előírások teljesítésének, valamint az érintettek jogai érvényesülésének elősegítése érdekében DPO-t alkalmaz.
(2) A DPO-t a Kancellár bízza meg határozatlan időtartamra.
(3) Adatvédelmi tisztviselőnek az nevezhető ki, aki
a) büntetlen előéletű és
b) a személyes adatok védelmére vonatkozó jogi előírások és jogalkalmazási gyakorlat megfelelő szintű ismeretével rendelkezik, valamint

c) alkalmas az ezzel járó feladatok ellátására, továbbá
d) jogi végzettséggel rendelkezik.
(4) Tevékenységéért a DPO-t havi rendszeres díjazás illeti meg.
(5) Amennyiben az adatvédelmi tisztviselői feladatok ellátása foglakoztatásra irányuló jogviszony keretében nem biztosítható, az adatvédelmi tisztviselői feladatok átmenetileg, az (1) bekezdése szerinti foglakoztatásra irányuló jogviszony létesítéséig külső megbízással is elláthatók. Ebben az esetben a jelen § rendelkezéseit azzal az eltéréssel kell alkalmazni, hogy a (3) bekezdésben írt feltételeknek a megbízási szerződésben kijelölt, személyes eljárásra köteles személynek kell megfelelnie.

### *Hatásköre*

95. §

(1) A DPO-t minden olyan vitás kérdésbe, amelyben a személyes adatok kezelése megjelenik kötelező bevonni.
(2) A DPO elősegíti az Egyetem – személyes adatok kezelésére vonatkozó jogi előírásokban meghatározott – kötelezettségeinek teljesítését, így különösen a következő feladatokat látja el:
a) Tájékoztat és szakmai tanácsot ad az Egyetem vagy az Egyetem által megbízott adatfeldolgozó részére a vonatkozó jogi előírásokkal kapcsolatban – konkrét ügyben írásos megkeresés alapján állásfoglalást készít, általános kérdésekben akár írásban (ideértve az elektronikus levelet is), akár szóban javaslatot fogalmaz meg.
b) Folyamatosan ellenőrzi a jogi előírásoknak és az Egyetem belső szabályainak való megfelelést adatvédelmi ellenőrzés keretében. A DPO adatvédelmi ellenőrzéseit az általa megállapított rendben, időközönként és területeken végzi.
c) Az adatvédelmi szabályok, illetve a vonatkozó belső szabályzók megsértése, megsértésének veszélye, továbbá más, a személyes adatokat érintő integritássértés esetén a DPO javaslatot tesz a jogsértés vagy a szabályok megsértésének megszüntetésére, a veszély elkerülésére vagy egyéb jellegű integritássértés orvoslására. A DPO szükség esetén tájékoztatja a kialakult helyzetről a Kancellárt, valamint segítséget nyújt, hatáskörén belül, a jogszerű állapot helyreállításához.
d) Szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését.
e) Együttműködik az Adatvédelmi Hatósággal. Az Adatvédelmi Hatósággal folytatott bármilyen levelezést, megkeresést előzetesen egyeztetni kell a DPO-val.
f) Véleményezi az adatkezelő által elkészített olyan belső szabályzókat, illetve azok módosítását, amelyek személyes adat kezeléséről rendelkeznek.
g) Tájékoztatja az érintetteket jogaikról és segítséget nyújt az érintettek jogérvényesítéséhez.
h) Kivizsgálja a hozzá érkezett bejelentéseket, adatvédelmi panaszokat, és a jogosulatlan adatkezelés észlelése esetén annak megszüntetésére, egyéb adatvédelmi integritássértés esetén pedig azok korrekciójára hívja fel az adatkezelőt vagy az adatfeldolgozót.
i) Segítséget nyújt az adatvédelmi ismeretek oktatásához, működésével növeli az adatvédelmi tudatosságot.
j) Teljesíti jelen Szabályzatban számára előírt nyilvántartás-vezetési kötelezettségeket.
k) Képviseli az Egyetemet az adatvédelmi tisztviselők konferenciáján.
l) Adatvédelmi kérdésekben, a Kancellár felkérése alapján, képviseli az Egyetemet.
m) Felügyeli az egészségügyi adatvédelmi tisztviselő munkáját.
n) Elvégzi jelen Szabályzat hiteles értelmezését.

(3) A DPO feladatait a beérkező kérések időrendi sorrendjében, és jelen Szabályzatban rögzített ügyintézési határidőn belül végzi, ugyanakkor, az adott adatkezelési műveletekhez (az adatkezelés jellegéhez, hatásköréhez, körülményéhez és céljához) fűződő kockázatot mérlegelve, önállóan priorizálhatja a feladatait.

### *Jogai és kötelezettségei*

96. §

(1) A DPO közvetlenül és kizárólag a Kancellárnak alárendelten, ugyanakkor függetlenül működik, feladatai ellátásával kapcsolatban utasításokat senkitől sem fogadhat el.
(2) A DPO-nak joga van tájékoztatást kérni bármely adatvédelmi integritássértés ügyének jelenlegi állásáról.
(3) A DPO feladatteljesítése érdekében az Egyetem bármely helyiségébe beléphet, bármely nyilvántartásba betekinthet, bármely adatkezelési folyamatot megismerhet, a Szabályzat hatálya alá tartozó személytől felvilágosítást kérhet adatvédelmi tárgykörben.
(4) Amennyiben az adott szervezeti egység az adatvédelmi megfelelőség tekintetében – a DPO-val való együttműködési kötelezettségére való figyelmeztetés után – nem működik együtt a DPO-val, a DPO köteles jelezni azt a Kancellár és a JII vezetője felé.
(5) Az Egyetem vagy az Egyetem adatfeldolgozója a DPO feladatai ellátásával összefüggő okból a DPO megbízatását nem vonhatja vissza, nem bocsáthatja el és szankcióval nem sújthatja, kivéve, ha olyan súlyos, vétkes magatartást tanúsít, amely alapján az általános munkajogi szabályok szerint azonnali hatályú felmondásnak lenne helye.
(6) A DPO-t feladatai teljesítésével kapcsolatban – a jogviszonya fennállása alatt és annak megszűnését követően is – titoktartási kötelezettség terheli, valamint a tudomására jutott személyes adatokat, információkat bizalmasan köteles kezelni.
(7) A DPO az általa elmondottakért, az általa javasoltakért, az általa végrehajtottakért felelősséggel tartozik. A DPO azonban felelősségre nem vonható az adott adatkezelést végző szervezeti egység vagy annak bármelyik munkatársának eljárásáért, mulasztásáért, vagy a javasoltak végrehajtásának minőségéért.

### *Összeférhetetlenség*

97. §

(1) A DPO adatvédelmi feladatai mellett más feladatokat is elláthat. A Kancellár biztosítja, hogy e feladatokból ne fakadjon összeférhetetlenség, továbbá, hogy az adatvédelmi feladataira a szervezet nagyságára és összetett működési profiljára tekintettel mindenkor elegendő idő álljon rendelkezésére.
(2) A DPO szabadon előzetes bejelentés nélkül végezhet
a) a szellemi alkotáshoz fűződő bármilyen tevékenységet (ideértve az oktatási tevékenységet, valamint a szerzői mű létrehozatalát),
b) az Egyetemen kívüli adatvédelmi tanácsadást, valamint adatvédelmi szakértői tevékenységet.
(3) A DPO előzetesen köteles bejelenteni a Kancellár és a JII vezetője felé, ha adatvédelmi panasz, adatvédelmi közérdekű bejelentés, adatvédelmi incidens vagy egyéb jellegű adatvédelmi integritássértés kivizsgálása esetén a vizsgálat alá vont személlyel hozzátartozói viszonyban áll.

### *Hivatalos kapcsolattartási adatai*

98. §

(1) A DPO postai és elektronikus levélcímét a JII az Egyetem honlapján keresztül hozza nyilvánosságra. A honlapon közzétett munkahelyi elérhetőségi adatok a hivatalos kapcsolattartási címek, a hivatalos ügymenet ezeken keresztül történik.
(2) A DPO nevét és kapcsolattartási adatait a közérdekű adatok között is fel kell tüntetni. A közzétételért a JII felelős.

### *Eljárási határidők*

99. §

(1) A megkereséseket a DPO a lehető legrövidebb időn belül kivizsgálja, és érdemben megválaszolja
a) az egyetem felsővezetőinek megkeresését, legkésőbb 10 napon belül;
b) a központi adatkezelést végző szervezeti egységek adatvédelmi referenseinek megkeresését, legkésőbb 20 napon belül;
c) az érintetti megkereséseket a GDPR-nak megfelelően, legkésőbb 28 napon belül;
d) az adatvédelmi tárgyú panaszokat és közérdekű bejelentéseket, legkésőbb 30 napon belül;
e) az egyéb megkereséseket, legkésőbb 40 napon belül.
(2) A megkeresésekre nyitva álló határidő meghosszabbítható a megkeresés tárgyát képező ügy összetettségére, a szükséges intézkedések megtételére, az ügy kivizsgálásába bevonni szükséges személyek mennyiségére, valamint az adott adatkezelés kockázatára tekintettel
a) az (1) bekezdés a), b) és e) szerint a meghosszabbított válaszadási határidő legfeljebb a válaszadásra eredetileg rendelkezésre álló időtartam kétszerese lehet.
b) az (1) bekezdés c) pontja szerinti érintetti megkeresés kapcsán a határidő további 60 nappal meghosszabbítható. A határidő meghosszabbításáról a DPO a késedelem okainak megjelölésével a kérelem kézhezvételétől számított 28 napon belül tájékoztatja az érintettet. Ha az Egyetem, mint adatkezelő nem tesz intézkedéseket az érintett kérelme nyomán, a DPO késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított 28 napon belül tájékoztatja az érintettet az intézkedés elmaradásának okairól, valamint arról, hogy az érintett panaszt nyújthat be valamely felügyeleti hatóságnál, és élhet bírósági jogorvoslati jogával.
c) az (1) bekezdés d) pontja szerinti panasz vagy közérdekű bejelentés elintézését megalapozó vizsgálat előreláthatólag 30 napnál hosszabb ideig tart, erről a panaszost vagy a közérdekű bejelentőt – az elintézés várható időpontjának és a vizsgálat meghosszabbítása indokainak egyidejű megjelölésével – tájékoztatni kell. A panasz vagy a közérdekű bejelentés elintézésének határideje ebben az esetben sem haladhatja meg a hat hónapot.
(3) A meghosszabbításról a DPO értesíti a megkeresést benyújtó személyt.

### *Jogi és Igazgatási Igazgatóság (JII)*

100. §

(1) Az Egyetem adatvédelmi feladatai elvégzésének operatív támogatását a JII segíti.
(2) A JII
a) vezeti a jelen Szabályzat szerinti nyilvántartásokat,
b) koordinálja az Egyetem adatvédelmi témájú weblapját,
c) segíti a központi adatkezelést végző szervezeti egységek vezetőit terhelő adatvédelmi megfelelést azzal, hogy az egységek vezetői által kijelölt adatvédelmi referenseket és azok helyetteseit informálja és munkájukat koordinálja,
d) ellátja a jelen Szabályzat szerinti egyéb feladatokat.
(3) A JII jogállásáról, összetételéről, irányításáról külön szabályzat rendelkezik.

### *Egészségügyi adatvédelmi tisztviselő*

101. §

(1) A KK elnökének javaslatára és a DPO egyetértésével az egészségügyi szolgáltatással, betegellátással kapcsolatosan, valamint az egészségügyi adatok védelmének megszervezésére és ellenőrzésére a Kancellár egészségügyi adatvédelmi tisztviselőt nevezhet ki, vagy bízhat meg.
(2) Az (1) bekezdés szerinti esetben az egészségügyi adatvédelmi tisztviselőt minden olyan vitás kérdésbe, amelyben az egészségügyi személyes adatok kezelése megjelenik, kötelező bevonni.
(3) Az egészségügyi adatvédelmi tisztviselő a DPO irányítása alatt végzi tevékenységét.
(4) Az egészségügyi adatvédelmi tisztviselő jogállására, feladat- és hatáskörére jelen Szabályzat rendelkezéseinek figyelembe vételével az Egyetem Egészségügyi Adatkezelési Eljárásrendje további előírásokat állapíthat meg.

## V. ZÁRÓ RENDELKEZÉSEK

102. §

(1) Jelen szabályzatot a Szegedi Tudományegyetem Szenátusa 2024. év április hó 29. napján tartott ülésén hozott SZ-348-VIII/2023/2024. (IV.29.) számú határozatával elfogadta.
(2) Jelen szabályzat 2024. év május hó 1. napján lép hatályba. Hatályba lépésével egyidejűleg a 2014. év július hó 07. napján elfogadott az SZTE Adatvédelmi, Közérdekű Adatmegismerési és Közzétételi Szabályzata hatályát veszti.
(3) A hatálybalépést követően a szabályzatban foglaltakat a már folyamatban lévő ügyekre nézve is alkalmazni kell.
(4) A szabályzat a következő linken érhető el folyamatosan: http://www.u-szeged.hu/szabalyzatok
(5) Az Egyetem szervezeti egységei a Szabályzat hatálybalépését követő 60 napon belül kötelesek felülvizsgálni saját kapcsolódó belső szabályozóikat, és azokat jelen szabályzatban írtakkal összhangban kötelesek módosítani.

**Kelt:** Szegeden, 2024. év április hó 29. napján

**Dr. Rovó László s. k.**
rektor

**Dr. Fendler Judit s.k.**
kancellár